



JPW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of)
YOSHIUCHI et al.)
Application Number: 10/766,189)
Filed: January 29, 2004)
For: CONNECTION CONTROL SYSTEM, CONNECTION)
CONTROL EQUIPMENT AND CONNECTION)
MANAGEMENT EQUIPMENT)
ATTORNEY DOCKET NO. ASAM.0104)

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

LETTER

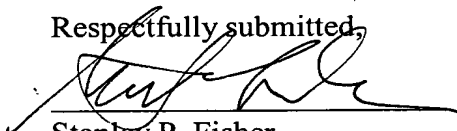
Sir:

The below-identified communications are submitted in the above-captioned application or proceeding:

- | | | |
|---|---------------------------|---|
| <input checked="" type="checkbox"/> (X) | Priority Documents (1) | |
| <input checked="" type="checkbox"/> (X) | Request for Priority | <input type="checkbox"/> () Assignment Document |
| <input type="checkbox"/> () | Response to Missing Parts | <input type="checkbox"/> () Petition under 37 C.F.R. 1.47(a) |
| | w/ signed Declaration | <input type="checkbox"/> () Check for \$130.00 |

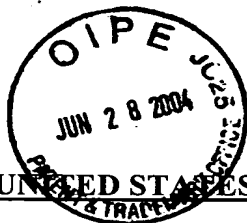
The Commissioner is hereby authorized to charge payment of any fees associated with this communication, including fees under 37 C.F.R. § 1.16 and 1.17 or credit any overpayment to **Deposit Account Number 08-1480**. A duplicate copy of this sheet is attached.

Respectfully submitted,


Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200
June 28, 2004



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of)
YOSHIUCHI et al.)
Application Number: 10/766,189)
Filed: January 29, 2004)
For: CONNECTION CONTROL SYSTEM, CONNECTION)
CONTROL EQUIPMENT AND CONNECTION)
MANAGEMENT EQUIPMENT)
ATTORNEY DOCKET NO. ASAM.0104)

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

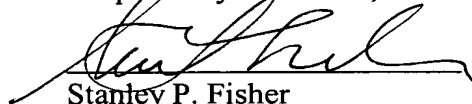
**REQUEST FOR PRIORITY
UNDER 35 U.S.C. § 119
AND THE INTERNATIONAL CONVENTION**

Sir:

In the matter of the above-captioned application for a United States patent, notice is hereby given that the Applicant claims the priority date of December 3, 2003, the filing date of the corresponding Japanese patent application 2003-403971.

A certified copy of Japanese patent application 2003-403971 is being submitted herewith. Acknowledgment of receipt of the certified copy is respectfully requested in due course.

Respectfully submitted,


Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200
June 28, 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 2 月 3 日
Date of Application:

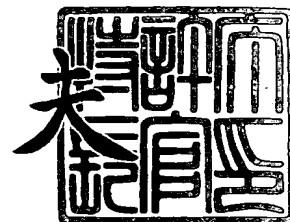
出 願 番 号 特 願 2 0 0 3 - 4 0 3 9 7 1
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 4 0 3 9 7 1]

出 願 人
Applicant(s): 株式会社日立製作所
 株式会社日立コミュニケーションテクノロジー

2 0 0 4 年 1 月 2 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 4 - 3 0 0 3 0 1 7

【書類名】 特許願
【整理番号】 H03008621A
【あて先】 特許庁長官 殿
【国際特許分類】 H04L 12/00
【発明者】
 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所
 中央研究所内
 【氏名】 吉内 英也
【発明者】
 【住所又は居所】 東京都品川区南大井六丁目 2 6 番 3 号 株式会社日立コミュニケー
 ーションテクノロジー内
 【氏名】 秋山 秀洋
【発明者】
 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所
 中央研究所内
 【氏名】 吉澤 政洋
【発明者】
 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所
 中央研究所内
 【氏名】 武田 幸子
【特許出願人】
 【識別番号】 000005108
 【氏名又は名称】 株式会社日立製作所
【特許出願人】
 【識別番号】 000153465
 【氏名又は名称】 株式会社日立コミュニケーションテクノロジー
【代理人】
 【識別番号】 100075096
 【弁理士】
 【氏名又は名称】 作田 康夫
 【電話番号】 03-3212-1111
【選任した代理人】
 【識別番号】 100100310
 【弁理士】
 【氏名又は名称】 井上 学
【手数料の表示】
 【予納台帳番号】 013088
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】特許請求の範囲**【請求項 1】**

通信網を介して第一及び第二の端末と接続可能な接続管理装置であって、
上記通信網に接続可能な送受信部と、
上記送受信部と接続され、さらに相互に接続されたCPU及びメモリとを備え、
上記送受信部で上記第一の端末から上記第二の端末への接続要求を受信した場合に、
上記CPUは、上記第一の端末から上記第二の端末への接続が可能かどうかを判定するプログラムを上記メモリから読み出して実行し、さらに上記CPUは、上記判定の結果、上記接続が不可能な場合には、上記第二の端末と接続可能なアドレスを生成するプログラムを上記メモリから読み出して実行し、
該生成されたアドレスを含むデータを上記送受信部から上記第一の端末へ送信することを特徴とする接続管理装置。

【請求項 2】

上記メモリには、上記第一の端末から上記第二の端末への接続が可能かどうかを判定するデータベースが格納されており、
上記CPUは、上記データベースを用いて上記判定を行うことを特徴とする請求項 1 記載の接続管理装置。

【請求項 3】

上記判定の結果、上記接続が不可能な場合には、
上記CPUはさらに、
上記第一の端末から上記第二の端末への通信経路を検索するプログラムを上記メモリから読み出して実行し、
上記検索の結果、上記通信経路が存在した場合に、上記アドレスを生成するプログラムを実行することを特徴とする請求項 1 記載の接続管理装置。

【請求項 4】

上記判定の結果、上記接続が不可能な場合には、第一の端末にその旨を通知し、
さらに上記第一の端末から要求があった後に、上記アドレスを生成することを特徴とする請求項 1 または 2 記載の接続管理装置。

【請求項 5】

上記判定の結果、上記接続が可能な場合には、
上記CPUはさらに、
上記第一の端末を認証するプログラムを上記メモリから読み出して実行し、
上記第一の端末の認証に成功した後に、上記アドレスを生成することを特徴とする請求項 1 乃至 3 のいずれかに記載の接続管理装置。

【請求項 6】

通信網を介して第一及び第二の端末と接続された接続制御システムであって、
上記通信網と接続された送受信部、上記送受信部と接続され、さらに互いに接続されたCPU及びメモリをそれぞれ備えた接続制御装置及びアドレス生成装置を備え、
上記接続制御装置では、
上記接続制御装置の送受信部で、上記第一の端末から上記第二の端末への接続要求を受付けた場合に、
上記接続制御装置のCPUが、上記第一の端末から上記第二の端末への接続が可能かどうかを判定するプログラムを上記接続制御装置のメモリから読み出して実行し、
上記判定の結果、上記接続が不可能な場合には、
上記接続制御装置の送受信部から、上記第二の端末と接続可能なアドレスの生成依頼を上記アドレス生成装置に送信し、
上記アドレス生成装置では、
上記アドレス生成装置の送受信部で、上記アドレスの生成依頼を受信し、
上記アドレス生成装置のCPUが上記第二の端末と接続可能なアドレスを生成するプログラムを上記アドレス生成装置のメモリから読み出して実行し、

上記アドレス生成装置の送受信部から、該アドレスを含むデータを上記第一の端末へ送信することを特徴とする接続制御システム。

【請求項 7】

上記接続制御装置での判定の結果、上記接続が不可能な場合には、
上記接続制御装置の CPU はさらに、上記第一の端末から上記第二の端末への通信経路を検索するプログラムを上記接続制御装置のメモリから読み出して実行し、
上記検索の結果、上記通信経路が存在した場合には、
上記接続制御装置の送受信部から、上記第二の端末と接続可能なアドレスの生成依頼を上記アドレス生成装置に送信することを特徴とする請求項 5 記載の接続制御システム。

【請求項 8】

上記接続制御装置における判定の結果、上記接続が不可能な場合には、
上記接続制御装置が第一の端末にその旨を通知し、
さらに上記第一の端末から要求があった後に、
上記アドレス生成装置が上記アドレスを生成することを特徴とする請求項 6 または 7 記載の接続制御システム。

【請求項 9】

上記通信網に接続された送受信部と、上記送受信部に接続され、さらに相互に接続された CPU 及びメモリを備えた認証装置をさらに備え、
上記接続制御装置における判定の結果、上記接続が可能な場合には、
上記認証装置の CPU は、上記第一の端末の認証を行うプログラムを上記認証装置のメモリから読み出して実行し、
さらに上記認証装置が上記第一の端末の認証に成功した後に、
上記アドレス生成装置が、上記アドレスを生成することを特徴とする請求項 1 乃至 3 のいずれかに記載の接続制御システム。

【請求項 10】

通信網を介して第一及び第二の端末、及びアドレス生成装置に接続された接続制御装置であって、
上記通信網と接続された送受信部と、
上記送受信部と接続され、さらに相互に接続された CPU 及びメモリを備え、
上記送受信部で、上記第一の端末から上記第二の端末への接続要求を受付けた場合に、
上記 CPU は、上記第一の端末から上記第二の端末への接続が可能かどうかを判定するためのプログラムを上記メモリから読み出して実行し、
上記判定の結果、上記接続が不可能な場合には、
上記送受信部から、上記第二の端末と接続可能なアドレスの生成依頼を上記アドレス生成装置に送信することを特徴とする接続制御装置。

【書類名】明細書**【発明の名称】**接続制御システム、接続制御装置、及び接続管理装置**【技術分野】****【0001】**

本発明は、通信網を介して複数の通信端末と相互接続されている接続制御システム、これを構成する接続制御装置、接続管理装置、この接続管理装置の動作プログラムに関する。

【背景技術】**【0002】**

通信網が拡大し、業務への適用が進む中、企業機密などの秘密情報を保護する目的で、接続に制限を設ける技術が開発されている。このような技術のうちで代表的なものは VPN (Virtual Private Network) である。VPNにはMPLS (Multi Protocol Label Switching)、IPSec (IP (Internet Protocol) Security protocol)、L2TP (Layer2 Tunneling Protocol) 等様々な技術を用いた実現方式が存在するが、基本動作は通信網に接続制限を設け、接続が許可されている通信網間に対してのみ通信を許可するというものである。接続許可はシステム構築時に接続許可データベースに接続を許可する接続元ネットワークと接続先ネットワークの対応を登録することで与えられる。多くの場合、接続許可を得るためには接続元端末と接続先端末が接続元ネットワーク、接続先ネットワークにそれぞれ属しているだけでは不十分であり、さらにユーザ認証、端末認証等の認証処理を必要とする。

【0003】

例えば、特許文献1には複数のISP (Internet Service Provider) 間にまたがるリモートVPNの統一的管理方法が記載されているが、このような場合にも認証処理を必要とする。

【0004】

【特許文献1】特開2003-8607号公報

【発明の開示】**【発明が解決しようとする課題】****【0005】**

しかし、前記の特許文献の接続制御方法では、接続元と接続先のISPが相互接続を許可していない場合など、接続元端末が接続許可のないネットワークに属する場合に通信できないという問題点がある。特に、移動体端末のように頻繁にネットワーク間を移動する端末では、自身が所属するネットワークが変化した場合に目的の端末と通信できなくなる可能性があるという問題が発生する。

本発明の目的は、接続に制限のあるネットワークにおいて、接続元端末または接続先端末の移動などにより接続元端末から接続先端末への接続が不可能となった場合に、接続元端末に対して接続先端末と通信が可能なアドレスを割り当てることにより、接続許可のない端末間の通信を実現することにある。

【課題を解決するための手段】**【0006】**

本発明における接続制御システムは、ネットワーク間または端末間の通信を制御し、接続許可判定を行う接続制御装置。接続要求を発した利用者を認証する認証装置を備える。接続許可のないネットワークに属する端末からの接続要求が到着した場合、接続制御システムは端末に対して接続ができない旨を通知する。さらに、端末が接続制御システムに対し、通信を可能にするための通信経路の検索と、通信の際に使用するアドレスの割当を要求した場合、接続制御システムは自システムが管理するネットワーク内で、迂回路通信経路を検索する。次に接続要求を発した端末の認証をした後、認証された端末に対して、接続許可のあるネットワークと接続可能なアドレスを割り当てることで前記問題を解決する。

【発明の効果】**【0007】**

本発明の接続制御システムは接続不可能な端末間の通信において、接続許可のあるネットワークの連結による迂回路を設定し、認証を経ることで接続許可のないネットワーク間の通信を可能にする。このような処理を行うことにより、頻繁にネットワークを移動する移動体端末同士の通信の利便性を向上させる。

【発明を実施するための最良の形態】**【0008】**

本発明における接続制御システムの構成を図1に示す。該システムにおいてネットワーク1(1)に属する端末1(10)、ネットワーク2(2)に属する端末2(20)、ネットワーク3(3)に属する端末3(30)、ネットワーク4(4)に属する端末4(40)は、LAN(50010)によりゲートウェイ1(15)、ゲートウェイ2(25)、ゲートウェイ3(35)、ゲートウェイ4(45)と接続し、これらを通じて、接続制御システム(5)に接続している。接続制御システム(5)は、端末間の通信を制御する接続制御装置(52)、利用者の認証を行う認証装置(54)、迂回路接続の際に必要な接続用アドレスを生成するアドレス管理装置(56)を備える。ここで、ネットワーク1(1)からネットワーク3(3)への通信は許可されていない。しかし、ネットワーク1(1)からネットワーク2(2)、ネットワーク2(2)からネットワーク3(3)への通信はそれぞれ許可されている。

【0009】

次に、接続制御システム(5)を構成する個々の要素の機能ブロックを示す。図2はゲートウェイ1(15)の構成である。接続制御装置が端末の接続を制御するために、接続制御装置と接続した図1中の他のゲートウェイ2~4(25、35、45)も同様の構成を持つ。

ゲートウェイ1(15)は、ネットワークインターフェース(50000)を通じて外部と通信を行う。ゲートウェイ1(15)はさらにCPU(50002)、ハードディスク(50004)、メモリ(50008)を備え、これらはバス(50006)により相互にデータを送受信する。これらのハードウェア構成において、ゲートウェイ1(15)は端末からのパケットを受信して、宛先アドレスへ送信するパケット送受信部(110)をネットワークインターフェース(50000)に、接続を許可された端末の実アドレス(12010)を登録するアドレス登録テーブル(120)、迂回路接続の際に使用する迂回路アドレス(13010)と実アドレス(13020)の組を登録する迂回路アドレス登録テーブル(130)、通信状態を監視する通信監視タイマ(140)をメモリ(50008)上に備える。

【0010】

実アドレスは端末のネットワークインターフェースに割り当てられているアドレスであり、接続元端末と接続先端末の通信が許可されている場合はこのアドレスを用いて通信を行う。迂回路接続とは接続元端末と接続先端末の通信ができない場合に、接続許可のあるネットワークを経由した通信経路を迂回路として用いることで端末間の接続を制御することを指す。迂回路アドレスは迂回路接続において通信を行う場合にアドレス管理装置が端末に割り当てたアドレスである。

図3は接続制御装置(52)の構成である。接続制御装置(52)は外部と通信するためのネットワークインターフェース(50000)と、CPU(50002)、ハードディスク(50004)、バス(50006)、メモリ(50008)を基本ハード構成として備える。さらに、接続制御装置(52)は端末からのパケットを受信、あるいは送信するためのパケット送受信部(520)、接続制御システム(5)内の他の装置に処理を依頼するためのメッセージを送信したり、他の装置の処理結果をメッセージとして受信するためのメッセージ送受信部(522)をネットワークインターフェース(50000)に、端末からの接続要求に対して送信元端末のアドレスと送信先端末のアドレスから接続許可を判定するための情報を含む接続許可データベース(524)をハードディスク(50

004) に、接続制御対象のユーザの状態を管理するユーザ状態管理部(526)、通信状態を監視する通信監視タイマ(528)をメモリ(50008)上で動作する接続制御プログラム(52000)の接続制御機能(52002)の一部として備える。ここで、メッセージとはシステム内の各装置間で交換されるパケットを指す。

【0011】

図4は接続許可データベース(524)の詳細である。接続許可データベース(524)は接続が許可されているネットワーク間の関係を保持するものであり、接続元ネットワーク(5242)、接続先ネットワーク(5244)と、迂回路として使用可能かどうかを示す迂回路判定フラグ(5246)を含む。迂回路判定フラグ(5246)が真の時は、この通信路を迂回路として用いることが可能である。

【0012】

図5はユーザ状態管理部(526)の詳細である。図5では一つのデータレコードのみ例示している。ユーザ状態管理部は接続制御中のユーザの状態を管理する機能ブロックであり、ユーザ名(5260)、端末アドレス(5261)、接続元ネットワーク(5262)、接続先ネットワーク(5264)、迂回路判定フラグ(5266)、認証判定フラグ(5268)、迂回路アドレス1(5270)、迂回路アドレスN(5272)を含む。迂回路判定フラグ(5266)は、対象ユーザが迂回路を使用中の場合に真となる。認証判定フラグ(5268)は、接続元ネットワークから接続先ネットワークへ通信する際のユーザ認証が完了済の場合に真となる。

【0013】

図6は認証装置(54)の構成である。認証装置(54)は外部と通信するためのネットワークインターフェース(50000)と、CPU(50002)、ハードディスク(50004)、バス(50006)、メモリ(50008)を基本ハード構成として備える。さらに、認証装置(54)はメッセージ送受信部(540)をネットワークインターフェース(50000)に、認証データベース(542)をハードディスク(50004)上に備え、メモリ(50008)上で動作する認証プログラム(54000)の認証機能(54002)の一部として通信監視タイマ(544)を備える。

【0014】

図7は認証データベース(542)の詳細である。図7では一つのデータレコードのみ例示している。迂回路接続を行う場合には複数の通信経路を経由して通信を行うが、その際認証は個々の通信経路ごとに行なう。認証データベース(542)は認証対象のユーザ名(5420)、接続元ネットワーク(5422)、接続先ネットワーク(5424)、パスワード(5426)を含む。

【0015】

図8はアドレス管理装置(56)の構成である。アドレス管理装置(56)は外部と通信するためのネットワークインターフェース(50000)と、CPU(50002)、ハードディスク(50004)、バス(50006)、メモリ(50008)を基本ハード構成として備える。さらに、アドレス管理装置(56)はメッセージ送受信部(560)をネットワークインターフェース(50000)に、迂回路接続に用いるアドレスを生成するアドレス生成部(562)、アドレス生成時に必要な情報を管理するネットワーク情報管理部(564)、通信状態を監視する通信監視タイマ(566)をメモリ(50008)上で動作するアドレス管理プログラム(56000)の接続制御機能(56002)の一部として備える。

【0016】

図9はネットワーク情報管理部(564)の詳細である。本発明における接続制御システムでは、通信プロトコルにIPv6を想定している。従って、迂回路用のアドレス生成にはネットワークを識別する識別子(5640)とネットワーク内で用いられているネットワーク接頭辞(5642)が必要である。IPv4を用いる場合には、アドレスの生成にはネットワーク接頭辞(5642)は必要ない。代わりに、ネットワーク内の端末のアドレスを管理し、未使用のアドレスを迂回路用のアドレスとして用いる必要がある。IP

v 4 におけるネットワーク情報管理部 (564) を図 26 に示す。ネットワーク情報管理部 (564) はネットワーク識別子 (5640) とアドレス管理データベース (5644) を備える。

【0017】

次に、該システムの動作をシーケンスを用いて詳述する。図 10 は接続制御システム (5) の基本シーケンスを示している。また、このシーケンスで用いられるパケットの内容を図 19 に示す。前述したように、接続制御システム (5) においてはネットワーク 1 (1) からネットワーク 2 (2)、ネットワーク 2 (2) からネットワーク 3 (3)、ネットワーク 3 (3) からネットワーク 4 (4)、への接続が許可されており、全ての接続が迂回路として使用可能であるものと仮定し、ネットワーク 1 (1) に属する端末 1 (10) がネットワーク 2 (2) に属する端末 2 (20) と通信する場合を考える。通信を始めるにあたり、端末 1 (10) はネットワーク 1 (1) からネットワーク 2 (2) への接続要求 (1000) をゲートウェイ 1 (15) を通じて送信する。以後特別な記述がない限り端末から接続制御装置 (52) への通信はゲートウェイを経由するものとする。接続要求 (1000) の内容を図 19 に示す。接続要求 (1000) は送信元 IP (2300)、宛先 IP (2302)、パケット種別 (接続要求) (2304)、接続元ネットワーク (2306)、接続先ネットワーク (2308)、ユーザ名 (2310) を情報として含む。接続要求 (1000) を受信した接続制御装置 (52) は、要求された接続が許可されているかどうかを接続許可データベース (524) に問い合わせる。接続許可データベース (524) は接続要求 (1000) の接続元ネットワーク (2306) とデータベース中の接続元ネットワーク (5242)、接続要求 (1000) の接続先ネットワーク (2308) とデータベース中の接続先ネットワーク (5244) を比較し、要求された接続が許可されているかどうかを判定する。次に接続制御装置 (52) はユーザ状態管理部 (526) に、該ユーザの認証が完了しているかどうかを問い合わせる。ユーザ状態管理部 (526) に該ユーザのエントリが存在しない場合には、接続制御装置 (52) は該ユーザのエントリを生成し、端末 1 (10) に認証要求 (1003) を送信する。図 19 に認証要求 (1003) の内容を示す。認証要求 (1003) は送信元 IP (2700)、宛先 IP (2702)、パケット種別 (認証要求) (2704)、接続元ネットワーク (2706)、接続先ネットワーク (2708)、ユーザ名 (2710) を情報として含む。該ユーザのエントリが存在する場合には、ユーザ状態管理部 (526) はエントリの認証判定フラグ (5268) を調べ、偽の場合には端末 1 (10) に認証要求 (1003) を送信する。端末 1 (10) はこれを受け、認証情報 (1006) を接続制御装置 (52) に送信する。認証情報 (1006) の内容を図 19 に示す。認証情報 (1006) は送信元 IP (2500)、宛先 IP (2502)、パケット種別 (認証情報) (2504)、接続元ネットワーク (2506)、接続先ネットワーク (2508)、ユーザ名 (2510)、パスワード (2512) を含む。認証情報 (1006) を受信した接続制御装置 (52) は、認証装置 (54) に認証依頼 (1009) を送信して認証を依頼する。認証依頼 (1009) の内容を図 19 に示す。認証依頼 (1009) はメッセージ種別 (認証依頼) (4300)、接続元ネットワーク (4302)、接続先ネットワーク (4304)、ユーザ名 (4306)、パスワード (4308) を含む。認証依頼 (1009) 中の接続元ネットワーク (4302)、接続先ネットワーク (4304)、ユーザ名 (4306)、パスワード (4308) の値は、認証情報 (1006) の接続元ネットワーク (2506)、接続先ネットワーク (2508)、ユーザ名 (2510)、パスワード (2512) から取得する。認証依頼 (1009) を受信した認証装置 (54) は、認証の成否を認証データベース (542) に問い合わせる。認証装置 (54) は認証依頼 (1009) 中の接続元ネットワーク (4302)、接続先ネットワーク (4304)、ユーザ名 (4306) を用いて認証データベース (542) から対応するデータレコードを検索し、認証依頼 (1009) 中のパスワード (4308) とデータレコード中のパスワード (5426) を比較する。パスワードが一致する場合には認証の完了を接続制御装置 (52) に通知する。これは認証完了 (1012) を送信することで行われる。認証完了 (101

2) を受けた接続制御装置 (52) は、認証完了通知 (1015) を端末 1 (10) に送信する。この時点で認証が完了するため、接続制御装置 (52) はユーザ状態管理部 (526) の認証要求 (1003) を送信したユーザの認証判定フラグ (5268) を真に、迂回路判定フラグ (5266) を偽に設定する。認証が完了した後に、接続制御装置 (52) はゲートウェイ 1 (15) に認証が完了したユーザのアドレス登録 (1016) を行う。アドレス登録 (1016) の内容を図 19 に示す。アドレス登録 (1016) は送信元 IP (5000)、宛先 IP (5002)、パケット種別 (アドレス登録) (5004)、実アドレス (5006) を含む。ゲートウェイ 1 (15) は実アドレス (5006) をアドレス登録テーブル (120) に登録する。

【0018】

ユーザ状態管理部 (526) 内のユーザ状態を更新した後、接続制御装置 (52) は接続許可通知 (1018) を端末 1 (10) に送信する。図 19 に接続許可通知 (1018) の内容を示す。接続許可通知 (1018) は送信元 IP (3300)、宛先 IP (3302)、パケット種別 (接続許可通知) (3304)、接続元ネットワーク (3306)、接続先ネットワーク (3308)、ユーザ名 (3310) を情報として含む。接続許可通知 (1018) を受信した端末 1 (10) はこの時点で端末 2 (20) との通信が可能になり、ゲートウェイ 1 (15)、ゲートウェイ 2 (25) を経由して端末 2 との通信を開始する (1021)。

端末 1 (10) は通信を終了する際に接続制御装置 (52) に対して接続終了 (1024) を送信する。接続終了 (1024) を受信した接続制御装置 (52) は、ユーザ状態管理部 (526) の該接続終了 (1024) を送信したユーザに対応するエントリを削除し、端末 1 (10) に接続終了確認 (1027) を送信する。最後に接続管理装置 (52) はゲートウェイ 1 (15) にアドレス削除 (1030) を送信する。アドレス削除 (1030) の内容を図 19 に示す。アドレス削除 (1030) は送信元 IP (5100)、宛先 IP (5102)、パケット種別 (アドレス削除) (5104)、実アドレス (5106) を含む。ゲートウェイ 1 (15) は実アドレス (5106) をアドレス登録テーブル (120) から削除する。以後端末 1 (10) が接続制御装置 (52) を経由して端末 2 (20) と通信するには、再度接続要求 (1000) を送信して認証を経なければならない。以上で通常の接続処理が完了する。

【0019】

次に、接続許可のないネットワーク間の通信について考える。図 12 はネットワーク 1 (1) からネットワーク 3 (3) への通信を要求した場合の処理である。図 1 においてネットワーク 2 (2) に属していた端末 2 (20) がネットワーク 1 (1) に移動して (9) 端末 1 (10) となり、ネットワーク 3 (3) に属する端末 3 (30) と通信する場合がこれに相当する。

【0020】

本発明におけるシステムでは迂回路を用いた通信を行うことで、接続許可のないネットワーク間では接続できないという問題を解決する。迂回路は接続許可がないネットワーク間の通信を実現するための通信経路である。図 1 において、ネットワーク 1 (1) からネットワーク 3 (3) への接続許可は存在しないが、ネットワーク 1 (1) からネットワーク 2 (2)、ネットワーク 2 (2) からネットワーク 3 (3) への接続許可は存在する。そこで、ネットワーク (1) からネットワーク (3) への通信を、ネットワーク 2 (2) を経由する迂回路を経ることで実現する。この時、接続許可を満たすアドレスを端末が持つことが必要となる。端末 1 がネットワーク 1 (1) からネットワーク 2 (2) を経由してネットワーク 3 (3) に属する端末 3 (30) と通信するには、ネットワーク 2 (2) からネットワーク (3) へ通信する必要があるが、接続許可を満たすためには端末 1 (10) がネットワーク 2 (2) におけるアドレスを持つ必要がある。ところが端末 1 (10) の持つアドレスはネットワーク (1) に属するため、そのままではネットワーク 2 (2) からネットワーク 3 (3) へ通信できない。そこで、アドレス管理装置 (56) は端末 1 (10) に迂回路アドレスとしてネットワーク 2 (2) でのアドレスを付与する。ネッ

トワーク 2 (2) における通信用のアドレスを端末に割り当てることで、ネットワーク 2 (2) を経由した、すなわち迂回路を用いた通信が可能になる。

【0021】

図 11 に迂回路を用いた通信シーケンスを示す。また、このシーケンスで用いられるパケットの内容を図 20、図 21 に示す。端末 1 (10) は接続制御装置 (52) に接続要求 (1200) を送信する。接続要求 (1200) を受信した接続制御装置 (52) は、要求された接続が許可されているかどうかを接続許可データベース (524) に問い合わせる。ネットワーク 1 (1) からネットワーク 3 (3) への通信は許可されていないため、接続制御装置 (52) は接続不許可通知 (1203) を端末 1 (10) に送信する。接続不許可通知 (1203) の内容を図 20 に示す。接続不許可通知 (1203) は送信元 IP (3500)、宛先 IP (3502)、パケット種別 (接続許可通知) (3504)、接続元ネットワーク (3506)、接続先ネットワーク (3508)、ユーザ名 (3510) を情報として含む。接続不許可通知 (1203) を受信した端末 (10) はネットワーク 1 (1) からネットワーク 3 (3) へ直接接続できないことを知り、接続制御装置 (52) に迂回路による接続を要求するため、迂回路接続要求 (1206) を送信する。迂回路接続要求の内容を図 20 に示す。迂回路接続要求 (1206) は送信元 IP (2400)、宛先 IP (2402)、パケット種別 (迂回路接続要求) (2404)、接続元ネットワーク (2406)、接続先ネットワーク (2408)、ユーザ名 (2410) を情報として含む。この例では接続元ネットワーク (2406) にネットワーク 1 (1)、接続先ネットワークにネットワーク 3 (3) を指定する。迂回路接続要求 (1206) を受信した接続制御装置 (52) は要求された迂回路が存在するかどうかを接続許可データベース (524) に問い合わせる。接続許可データベース (524) は迂回路接続要求 (1200) の接続元ネットワーク (2406) と接続先ネットワーク (2408) を用いて迂回路を検索する。接続許可データベース (524) は、接続元ネットワークから接続先ネットワークを結ぶ経路が、自身が管理する接続許可のあるネットワークの連結で構築できる場合に迂回可能と判断する。ネットワークの連結とは、ある接続許可 1 の接続先ネットワークと別の接続許可 2 の接続元ネットワークが一致する場合に、接続許可 1 の接続元ネットワークを接続元ネットワークに、接続許可 2 の接続先ネットワークを接続先ネットワークにした新しい接続許可 3 を生成することを指す。例えば、ネットワーク 1 (1) からネットワーク 3 (3) については、接続許可データベース中の接続許可のうちネットワーク 1 (1) からネットワーク 2 (2)、ネットワーク 2 (2) からネットワーク 3 (3) という経路が存在し、ネットワークの連結による迂回が可能である。可能と判断したら、接続制御装置 (52) はユーザ状態管理部 (526) に、迂回路接続要求 (1206) を送信したユーザの認証が完了しているかどうかを問い合わせる。この時点ではユーザ状態管理部 (526) には該ユーザのエントリはまだ生成されていないので、接続制御装置 (52) は該ユーザのエントリを生成し、端末 1 (10) に迂回路認証要求 (1209) を送信する。図 20 に迂回路認証要求 (1209) の内容を示す。迂回路認証要求 (1209) は送信元 IP (2800)、宛先 IP (2802)、パケット種別 (迂回路認証要求) (2804)、接続元ネットワーク (2806)、経由ネットワーク 1 (2808)、経由ネットワーク N (2810)、接続先ネットワーク (2812)、ユーザ名 (2814) を情報として含む。N は N 番目の経由ネットワークを表わす。この例ではネットワーク 2 (2) を経由するので、接続元ネットワーク (2806) にネットワーク 1 (1)、経由ネットワーク 1 (2808) にネットワーク 2 (2)、接続先ネットワーク (2812) にネットワーク 3 (3) を指定する。ネットワークの指定には各ネットワークが識別できる情報を用いる。例えば各ネットワークに属するゲートウェイのアドレスや、アドレス管理装置 (56) のネットワーク情報管理部 (564) が持つネットワーク識別子 (5640) 等がこれに相当する。迂回路認証要求 (1209) を受信した端末 1 (10) は迂回路認証情報 (1212) を接続制御装置 (52) に送信する。迂回路認証情報 (1212) は経由する全ての迂回路に必要な認証情報を含む必要がある。迂回路認証情報 (1212) の内容を図 20 に示す。迂回路認証情報 (1212) は送信元 IP (

2600)、宛先IP(2602)、パケット種別(迂回路認証情報)(2604)、接続元ネットワーク(2606)、経由ネットワーク1(2608)、経由ネットワークN(2610)、接続先ネットワーク(2612)、ユーザ名(2614)、パスワード1(2616)、パスワードN+1(2618)を含む。パスワードIは経由ネットワークI-1から経由ネットワークIへ接続する際に必要なパスワードを表す。経由ネットワーク0は接続元ネットワーク(2608)、経由ネットワークN+1は接続先ネットワーク(2610)に対応する。迂回路認証情報(1212)を受信した接続制御装置(52)は、認証装置(54)に迂回路認証依頼(1215)を送信して認証を依頼する。迂回路認証依頼(1215)の内容を図20に示す。迂回路認証依頼(1215)はメッセージ種別(迂回路認証依頼)(4400)、接続元ネットワーク(4402)、経由ネットワーク1(4404)、経由ネットワークN(4406)、接続先ネットワーク(4408)、ユーザ名(4410)、パスワード1(4412)、パスワードN+1(4414)を含む。経由ネットワークとパスワードの添字の関係は迂回路認証情報(1212)と同様である。迂回路認証依頼(1215)を受信した認証装置(54)は、認証の成否を認証データベース(542)に問い合わせる。認証装置(54)は迂回路認証依頼(1215)中の全てのパスワードに対して経由ネットワークI-1、経由ネットワークI、ユーザ名(4410)、パスワードIを、認証データベース(542)の接続元ネットワーク(5422)、接続先ネットワーク(5424)、ユーザ名(5420)、パスワード(5426)とそれぞれ比較し、全てのパスワードに対してデータレコードが存在する場合に認証の完了を接続制御装置(52)に通知する。これは迂回路認証完了(1218)を送信することで行われる。迂回路認証完了(1218)の内容を図20に示す。迂回路認証完了(1218)はメッセージ種別(迂回路認証完了)(3900)、接続元ネットワーク(3902)、経由ネットワーク1(3904)、経由ネットワークN(3906)、接続先ネットワーク(3908)、ユーザ名(3910)を情報として含む。迂回路認証完了(1218)を受けた接続制御装置(52)は、迂回路認証完了通知(1221)を端末1(10)に送信する。迂回路認証完了通知(1221)の内容を図21に示す。迂回路認証完了通知(1221)は送信元IP(3000)、宛先IP(3002)、パケット種別(迂回路認証完了通知)(3004)、接続元ネットワーク(3006)、経由ネットワーク1(3008)、経由ネットワークN(3010)、接続先ネットワーク(3012)、ユーザ名(3014)を情報として含む。この時点で認証が完了するため、接続制御装置(52)はユーザ状態管理部(526)の該ユーザの認証判定フラグ(5268)と迂回路判定フラグ(5266)を真に設定する。先述したように、迂回路接続の際にはそれぞれの経由ネットワークに対して端末の迂回路アドレスを生成する必要がある。接続制御装置(52)は迂回路アドレスの生成をアドレス管理装置(56)に依頼する。この処理はアドレス生成依頼(1224)をアドレス管理装置(56)に送信することで行う。アドレス生成依頼(1224)の内容を図21に示す。アドレス生成依頼(1224)はメッセージ種別(アドレス生成依頼)(4500)、端末MACアドレス(4502)、経由ネットワーク1(4504)、経由ネットワークN(4506)を情報として含む。端末のMACアドレスは、ユーザ状態管理部(526)の端末アドレス(5261)から抽出可能であり、アドレス生成を依頼する際にアドレス管理装置(56)にこれを送信する。アドレス生成依頼(1224)を受信したアドレス管理装置(56)はアドレス生成処理を行う。アドレスの生成は受信したアドレス生成依頼(1224)中の端末MACアドレス(4502)と、経由ネットワークIのゲートウェイのアドレスから検出したネットワークプレフィックスネットワーク接頭辞(5642)を用いて行う。IPv4の場合はアドレス管理データベース(5644)を検索して未使用のアドレスを生成アドレスとして用いる。アドレス管理装置(56)は生成したアドレスをアドレス生成完了(1227)を用いて接続制御装置(52)に通知する。アドレス生成完了(1227)の内容を図21に示す。アドレス生成完了(1227)はメッセージ種別(アドレス生成完了)(4200)、端末MACアドレス(4202)、生成アドレス1(4204)、生成アドレスN(4206)を情報として含む。生成アドレスIはアドレス生成

依頼(1224)の経路ネットワークIに対応したアドレスである。アドレス生成完了(1227)を受信した接続制御装置(52)はアドレスをユーザ状態管理部(526)の迂回路アドレスに登録する。ここではネットワーク2(2)用の迂回路アドレスを迂回路アドレス1(5270)として登録する。次に、アドレス生成通知(1230)を端末1(10)に送信して生成したアドレスを通知する。アドレス生成通知(1230)の内容を図21に示す。アドレス生成通知(1230)は送信元IP(3700)、宛先IP(3702)、パケット種別(アドレス生成通知)(3704)、端末アドレス(3706)、生成アドレス1(3708)、生成アドレスN(3710)を情報として含む。端末1(10)はネットワーク2(2)用のアドレスを受信し、以降の通信に用いる。この処理については後述する。端末1(10)へのアドレスの通知を終えた接続制御装置(52)は、迂回路接続を可能にするために通信路上に存在するゲートウェイに対してアドレスの登録を行う。通信路に存在するゲートウェイにはゲートウェイ1(15)、ゲートウェイ2(25)、ゲートウェイ3(35)があるが、ここではゲートウェイ1(15)に接続許可のために必要なアドレスの登録、ゲートウェイ2(25)に迂回路通信のために必要なアドレスの登録をそれぞれ行う。接続制御装置(52)はゲートウェイ1(15)にアドレス登録(1231)を送信する。ここで登録するアドレスは端末1(10)のアドレスであり、これはユーザ状態管理部(526)の端末アドレス(5261)に格納されている。次に接続制御装置(52)は迂回路アドレス登録(1232)をゲートウェイ2(25)に送信する。図21に迂回路アドレス登録(1232)の内容を示す。迂回路アドレス登録(1232)は送信元IP(5200)、宛先IP(5202)、パケット種別(迂回路アドレス登録)(5204)、迂回路アドレス(5206)、実アドレス(5208)を情報として含む。迂回路アドレス(5206)は接続先ネットワークに存在する端末が迂回路ネットワークに後続のパケットを送信するために必要なアドレスであり、この例ではネットワーク2(2)に対して生成したアドレスが該当する。実アドレス(5208)は経路ネットワークに存在するゲートウェイが後続のパケットを転送するために必要なアドレスであり、一つ前の経路ネットワークに対して生成したアドレスが該当する。つまり、ネットワークIを経由する場合、迂回路アドレスにはネットワークIに対して生成したアドレス、実アドレスにはネットワークI-1に対して生成したアドレスが該当する。なお、ネットワーク1は端末が属するネットワークである。ここでは迂回路アドレス(5206)にネットワーク2(2)用のアドレスを指定する。これはユーザ状態管理部(526)の迂回路アドレス1(5270)に格納されている。実アドレス(5208)

には端末1(10)のアドレスを指定する。これはユーザ状態管理部(526)の端末アドレス(5261)に格納されている。必要なアドレスの登録を終えた接続制御装置(52)は、端末1(10)に迂回路接続許可通知(1233)を送信する。迂回路接続許可通知(1233)の内容を図21に示す。迂回路接続許可通知(1233)は送信元IP(3400)、宛先IP(3402)、パケット種別(迂回路接続許可通知)(3404)、接続元ネットワーク(3406)、経路ネットワーク1(3408)、経路ネットワークN(3410)、接続先ネットワーク(3412)、ユーザ名(3414)を情報として含む。迂回路接続許可通知(1233)を受信した端末はゲートウェイ1(15)、ゲートウェイ2(25)、ゲートウェイ3(35)を経由して端末3(30)との通信を行う(1236)。

【0022】

端末1(10)は通信を終了する際に接続制御装置(52)に対して接続終了(1239)を送信する。接続終了(1239)を受信した接続制御装置(52)は、ユーザ状態管理部(526)の該接続終了(1239)を送信したユーザに対応するエントリを削除し、端末1(10)に接続終了確認(1242)を送信する。最後に接続管理装置(52)はゲートウェイに登録したアドレスを削除するために、ゲートウェイ1(15)にアドレス削除(1245)を送信する。アドレス削除(1245)の内容は、図19に示したアドレス削除(1030)の内容と同様である。ゲートウェイ1(15)は実アドレス(

5106) をアドレス登録テーブル (120) から削除し、以後端末 1 (10) が接続制御装置 (52) を経由して端末 3 (30) と迂回路接続による通信をするには、再度迂回路接続要求 (1206) を送信して認証を経なければならない。次に接続制御装置 (52) はゲートウェイ 2 (25) に迂回路アドレス削除 (1248) を送信する。迂回路アドレス削除 (1248) の内容を図 21 に示す。迂回路アドレス削除 (1248) は送信元 IP (5300)、宛先 IP (5302)、パケット種別 (迂回路アドレス削除) (5304)、迂回路アドレス (5306)、実アドレス (5308) を情報として含む。以上で迂回路接続処理が完了する。

【0023】

次に、各機能ブロックの動作をフローチャートを用いて詳述する。

図 12 は接続制御装置 (52) のフローチャートである。接続制御装置 (52) はシステム起動時に処理を開始して (1300) メッセージ/パケット受信ループに入る (1301)。受信したメッセージが接続要求 (1000) の場合 (1302)、接続制御装置 (52) は接続処理 (1324) を行う。接続処理 (1324) については後述する。受信したメッセージが迂回路接続要求 (1206) の場合 (1304)、接続制御装置 (52) は迂回路接続処理 (1326) を行う。迂回路接続処理 (1326) については後述する。認証情報 (1006) を受信した場合 (1306)、接続制御装置 (52) は認証装置 (54) に認証を依頼する (1328)。迂回路認証情報 (1212) を受信した場合 (1308)、接続制御装置 (52) は認証装置 (54) に迂回路認証を依頼する (1330)。認証失敗を受信した場合 (1310)、接続制御装置 (52) は端末に認証失敗を通知する (1332)。認証失敗は認証装置 (54) が認証に失敗したことを接続制御装置 (52) に通知するメッセージである。迂回路認証失敗を受信した場合 (1312)、接続制御装置 (52) は端末に迂回路認証失敗を通知する (1334)。迂回路認証失敗は認証装置 (54) が迂回路認証に失敗したことを接続制御装置 (52) に通知するメッセージである。迂回路認証失敗の内容を図 22 に示す。迂回路認証失敗はメッセージ種別 (迂回路認証失敗) (4100)、接続元ネットワーク (4102)、経由ネットワーク 1 (4104)、経由ネットワーク N (4106)、接続先ネットワーク (4108)、ユーザ名 (4110) を情報として含む。接続制御装置は端末に迂回路認証失敗通知を送信する。迂回路認証失敗通知の内容を図 22 に示す。迂回路認証失敗通知は送信元 IP (3200)、宛先 IP (3202)、パケット種別 (迂回路認証失敗通知) (3204)、接続元ネットワーク (3206)、経由ネットワーク 1 (3208)、経由ネットワーク N (3210)、接続先ネットワーク (3212)、ユーザ名 (3214) を情報として含む。認証完了 (1012) を受信した場合 (1314)、接続制御装置 (52) は認証完了通知 (1015) を端末に送信して認証完了を通知し (1336)、ゲートウェイにアドレス登録 (1030) を送信してアドレス登録テーブル (120) に端末のアドレスを登録し (1338)、接続許可通知 (1018) を端末に送信して通信を開始させる (1340)。迂回路認証完了 (1218) を受信した場合 (1316)、接続制御装置 (52) は迂回路認証完了通知 (1221) を端末に送信して迂回路認証完了を通知し (1342)、アドレス管理装置にアドレス生成依頼 (1224) を送信してアドレスの生成を依頼する (1344)。アドレス生成完了 (1227) を受信した場合 (1318)、接続制御装置 (52) はアドレス生成通知 (1230) を端末に送信し (1346)、端末のアドレスと生成した迂回路アドレスをアドレス登録 (1231)、迂回路アドレス登録 (1232) によりゲートウェイに登録し (1348)、迂回路接続許可通知 (1233) を端末に送信する (1350)。端末から接続終了 (1239) を受信した場合 (1320)、接続制御装置 (52) は接続終了確認 (1242) を端末に送信し (1352)、アドレス削除 (1245)、迂回路アドレス削除 (1248) によりゲートウェイから該当するアドレスを削除する (1354)。パケット/メッセージ受信ループはシステム停止時に停止して (1322)、接続制御装置 (52) は終了する (1399)。

【0024】

次に接続処理の様子を図 13 に示す。接続処理が開始すると (1400)、最初に要求

された接続が許可されているかどうかを把握するために、接続許可データベース(524)を検索する(1402)。対応するデータレコードが接続許可データベース(524)に存在しなければ、接続制御装置(52)は接続不許可通知(1203)を端末に送信して(1420)接続処理を終了する(1499)。データレコードが存在する場合はユーザ状態管理部(526)を検索して認証が完了しているかどうかを調べる(1404)。認証が完了していない場合は認証要求(1003)を端末に送信して(1422)接続処理を終了する(1499)。認証が完了している場合は接続許可通知(1018)を送信して(1406)接続処理を終了する(1499)。

【0025】

次に迂回路接続処理の様子を図14に示す。迂回路接続処理が開始すると(1500)、最初に要求された迂回路が存在するかどうかを把握するために、接続許可データベース(524)を検索する(1502)。迂回路が接続許可データベース(524)から算出できない場合、接続制御装置(52)は迂回路接続不許可通知を端末に送信して(1520)接続処理を終了する(1599)。迂回路接続不許可通知の内容を図22に示す。迂回路接続不許可通知は送信元IP(3600)、宛先IP(3602)、パケット種別(迂回路接続許可通知)(3604)、接続元ネットワーク(3606)、接続先ネットワーク(3608)、ユーザ名(3610)を情報として含む。迂回路が存在する場合はユーザ状態管理部(526)を検索して認証が完了しているかどうかを調べる(1504)。認証が完了していない場合は迂回路認証要求(1209)を端末に送信して(1522)接続処理を終了する(1599)。認証が完了している場合はアドレスが生成済であるかどうかをユーザ状態管理部(526)に問い合わせる。アドレス生成判定は迂回路判定フラグ(5266)が真の場合に迂回路アドレス1(5270)が存在するかどうかによって行う。アドレスが未生成の場合、接続制御装置(52)はアドレス管理装置(56)にアドレス生成依頼(1224)を送信する(1524)。アドレスが生成済の場合は端末にアドレス生成通知(1230)を送信してアドレスの通知を行い(1508)、迂回路接続許可通知(1233)を送信して(1510)迂回路接続処理を終了する(1599)。

【0026】

図15は認証装置(54)のフローチャートである。認証装置(54)はシステム起動時に処理を開始して(1600)メッセージ受信ループに入る(1601)。受信したメッセージが認証依頼(1009)の場合(1602)、認証装置(54)は認証処理を行う(1620)。認証処理については後述する。受信したメッセージが迂回路認証依頼(1215)の場合(1604)、認証装置(54)は迂回路認証処理を行う(1622)。メッセージ受信ループはシステム停止時に停止して(1606)、認証装置は終了する(1699)。

【0027】

次に認証処理の様子を図16に示す。認証処理が開始すると(1700)、最初に認証情報中のユーザ名が認証データベース(542)に存在するかを検索する(1702)。ユーザ名が存在しない場合、認証装置(54)は認証失敗を接続制御装置(52)に送信して(1720)処理を終了する(1799)。ユーザ名が存在する場合はパスワードが正当かどうかを検索する(1704)。パスワードが不正な場合は認証装置(54)は認証失敗を接続制御装置(52)に送信して(1722)処理を終了する(1799)。パスワードが正当な場合は認証装置(54)は認証完了(1012)を接続制御装置(52)に送信して(1706)処理を終了する(1799)。

【0028】

次に迂回路認証処理の様子を図17に示す。迂回路認証処理が開始すると(1800)、最初に認証情報中のユーザ名が認証データベース(542)に存在するかを検索する(1802)。ユーザ名が存在しない場合、認証装置(54)は迂回路認証失敗を接続制御装置(52)に送信して(1820)処理を終了する(1899)。ユーザ名が存在する場合はパスワードが正当かどうかを検索する(1804)。迂回路認証に必要な全てのパス

ワードが正当な場合にのみパスワードが正当であるとみなす。パスワードが不正な場合は認証装置(54)は迂回路認証失敗を接続制御装置(52)に送信して(1822)処理を終了する(1899)。パスワードが正当な場合は認証装置(54)は迂回路認証完了(1218)を接続制御装置(52)に送信して(1806)処理を終了する(1899)。

【0029】

図18はアドレス管理装置(56)のフローチャートである。アドレス管理装置(56)はシステム起動時に処理を開始して(1900)メッセージ受信ループに入る(1901)。アドレス管理装置はアドレス生成依頼(1224)を受信すると(1902)、メッセージ中の端末MACアドレス(4502)、経由ネットワーク1(4504)、経由ネットワークN(4506)から迂回路接続用のアドレスを生成し(1904)、アドレス生成完了(1227)を接続制御装置(52)に送信する(1906)。メッセージ受信ループはシステム停止時に停止して(1908)、アドレス管理装置は終了する(1999)。

【0030】

次に、端末1(10)が端末3(30)に対して通信を行う際の packets 処理について説明する。図27は端末1(10)が端末3(30)に通信する際のシーケンスである。図11において端末1(10)がアドレス生成通知(1230)を受信した時点で、端末1(10)は迂回路ネットワーク1であるネットワーク2(2)用のアドレスを保持する。端末1(10)が最初に保持するアドレスをHost1と記述し、ネットワーク2(2)用の迂回路アドレスをHost1-2と記述する。アドレス登録(1231)をゲートウェイ1(15)が受信すると、ゲートウェイ1(15)のアドレス登録テーブル(120)にはHost1が登録され、端末1(10)がゲートウェイ1(15)経由で通信することが可能になる。ゲートウェイ2(25)が迂回路アドレス登録(1232)を受信すると、ゲートウェイ2(25)の迂回路アドレス登録テーブル(130)には迂回路アドレス(13010)としてHost1-2、実アドレス(13020)としてHost1が登録される。これらの情報は迂回路接続において、端末3から端末1への packets を送信する際に必要となる。端末1(10)が迂回路接続許可通知(1233)を受信すると、端末1(10)は通信がゲートウェイ1、2、3を経由して送信されることを知る。端末1(10)は端末3(30)へ packets を以下の手順で送信する。端末1(10)は最初にゲートウェイ1(15)に packets (5498)を送信する(5499)。端末1(10)がゲートウェイ1(15)に送信する packets (5498)は packets の真の始点(5408)、真の終点(5410)、トンネル通信の始点(5400)、トンネル通信の終点(5402)、迂回ヘッダ1(5404)、迂回ヘッダ2(5406)とペイロード(5412)を含む。端末1(10)から端末3(30)への通信は最初にゲートウェイ1(15)を経由するので、トンネル通信の始点にHost1(5450)、終点にGW1(5452)を指定する。GW1はゲートウェイ1(15)のアドレスであり、これは迂回路接続許可通知(1233)の接続元ネットワーク(3406)に含まれている。接続許可を満たすために、packets はゲートウェイ2(25)、ゲートウェイ3(35)を経由しなければならない。これを実現するため、端末1(10)は packets 中に2つの迂回ヘッダを挿入する。迂回ヘッダは送信元と送信先を対にして指定する。ここではゲートウェイ1(15)からゲートウェイ2(25)への迂回ヘッダ(5454)、ゲートウェイ2(25)からゲートウェイ3(35)への迂回ヘッダ(5456)をそれぞれ指定する。packets の真の終点には端末3(30)のアドレスであるHost3を指定するが、ここで問題となるのは真の始点である。端末3が packets を受信した時、packets を返信する際にはネットワーク3(3)から接続許可のあるネットワークに対してのみ返信が可能である。そこで、真の始点にはネットワーク2用の迂回アドレスHost1-2を指定する。迂回アドレスは終点に対して必ず接続許可があるように算出されているため、真の始点に迂回アドレスを指定することで端末3(30)からの packets 返送が可能になる。ペイロード(5412)には端末3(30)へ送信したいデータ(5462)を

含める。端末1からのパケット(5498)を受信したゲートウェイ1(15)は以下の手順でパケットを処理する。トンネル通信の始点(5400)と終点(5402)から、トンネル通信の終点が自分自身であることを把握してこれらを取り除く。次にゲートウェイ1(15)は迂回ヘッダの検索を行う。端末1(10)がゲートウェイ1(15)に送信したパケット(5498)にはゲートウェイ1(15)からゲートウェイ2(25)への迂回を要求する迂回ヘッダ1(5404)が存在するので、トンネル通信の始点をGW1に(5550)、終点をGW2に指定し(5552)、迂回ヘッダを一つ取り除いてゲートウェイ2からゲートウェイ3への迂回ヘッダのみを指定する(5554)。真の始点(5506)、真の終点(5508)、ペイロード(5510)は元のパケットのデータをそのままコピーする(5556、5558、5560)。以上の処理を経てゲートウェイ1(15)はゲートウェイ2(25)にパケット(5598)を送信する(5599)。このパケットを受信したゲートウェイ2(25)はゲートウェイ1(15)と同様の処理を行い、ゲートウェイ3(35)にパケット(5698)を送信する(5699)。トンネル通信の始点はGW2(5650)、終点はGW3(5652)、真の始点はHost1-2(5654)、真の終点はHost3(5656)である。ペイロード(5658)は変化しない。このパケットを受信したゲートウェイ3(35)はパケットを解析し、迂回ヘッダが存在しないことを知る。従って、ゲートウェイ3(35)はゲートウェイ2(25)から受信したパケットをトンネル化せずに通常の通信として処理する。パケットの真の終点はHost3であるため、ゲートウェイ3(35)は図26に示すパケットを構築する。パケットの始点はHost1-2(5750)、終点はHost3(5752)である。ペイロード(5754)は変化しない。このようにして構築したパケット(5798)が端末3(30)に到達する(5799)。

次に端末3(30)から端末1(10)へのパケットの返送について説明する。端末3が把握しているパケットの送信元は、ゲートウェイ3(35)から受信したパケット(5798)の始点(5700)で指定されたHost1-2(5750)である。この情報を元にして端末3(30)は端末1(10)へのパケット(5898)を構築する。端末3(30)はパケットを真の始点をHost3(5854)、真の終点をHost1-2(5856)に設定し、トンネルの始点をHost3(5850)、トンネルの終点をGW3(5852)に設定する。このパケットを受信したゲートウェイ3(35)は(5899)、パケットの真の終点がHost1-2であることから、ゲートウェイ1(15)に送信する(5999)パケット(5998)を構築する。真の始点(5904)、真の終点(5906)、ペイロード(5908)は変化しない。トンネルの始点はGW3(5950)、トンネルの終点はGW2(5952)に設定される。このパケットを受信したゲートウェイ2(25)はネットワーク2(2)の中でパケットの転送先を検索するが、Host1-2は端末1(10)がネットワーク2(2)内で用いる仮想的なアドレスのため、パケットの転送先は存在しない。そこでゲートウェイ2(25)は迂回路アドレス登録テーブル(130)を検索し、該当する迂回路が存在しないかどうか調べる。ゲートウェイ2(25)の迂回路アドレス登録テーブル(130)には迂回路アドレス(13010)としてHost1-2、実アドレス(13020)としてHost1が登録されているので、ゲートウェイ2(25)はパケットをゲートウェイ1(15)に送信する。以上の情報を元にゲートウェイ2(25)はパケット(6098)をゲートウェイ1(15)に送信する(6099)。トンネルの始点(6050)はGW2、トンネルの終点はGW1(6052)に設定される。真の始点はHost3のまま変化しない(6054)が、真の終点は迂回路アドレス登録テーブル(130)から抽出した実アドレス(13020)であるHost1に変化する(6056)。ゲートウェイ2(25)からのパケット(6098)を受信したゲートウェイ1(15)はパケットの終点がHost1であることを知り、パケット(6198)を構築して端末1(10)に送信する(6199)。このパケットは始点がHost3(6150)、終点がHost1(6152)に設定されている。以上の処理を経て端末3(30)から端末1(10)にパケットが返送される。

【0031】

次に、接続制御システムを一つの接続管理装置（6）として実現した場合の構成を図23に示す。接続管理装置（6）はネットワークインターフェース（50000）とバス（50006）、メモリ（50008）を最低限備える。接続管理装置（6）の構成については図25で詳述する。接続管理装置（6）はメモリ（50008）上で動作する接続管理プログラム（60000）の機能として接続制御機能（60002）、認証機能（60004）、アドレス管理機能（60006）を備える。各機能は接続制御装置（52）、認証装置（54）、アドレス管理装置（56）と同等の機能を提供し、処理シーケンスは図10、図11と同様である。

次に、図24を用いてシステムのハードウェア構成を示す。図1で示したように、接続制御システム（5）は接続制御装置（52）、認証装置（54）とアドレス管理装置（56）から成る。これらの装置はそれぞれネットワークインターフェース（50000）を備え、LAN（50010）によって相互に通信を行う。各装置はそのほかにCPU（50002）、ハードディスク（50004）、メモリ（50008）を備え、これらは装置内のバス（50006）によって相互にデータを送受信する。各装置のメモリ（50008）にはそれぞれの装置の機能を実現するプログラムが格納されている。接続制御装置（52）のメモリ（50008）上では接続制御プログラム（52000）が動作、このプログラムは接続制御機能（52002）を備える。同様に、認証装置（54）のメモリ（50008）上では認証機能（54002）を備えた認証プログラム（54000）が、アドレス管理装置（56）のメモリ（50008）上ではアドレス管理機能（56002）を備えたアドレス管理プログラム（56000）が動作する。これらの装置の実現形態としては、各装置に個別のコンピュータを割り当てるほかに、ブレードサーバのように複数のコンピュータを単一の筐体として扱える形で実現することもできる。また、単一のコンピュータに全ての機能を実装することも可能である。図25に単一のハードウェアでの接続管理装置（6）の実装を示す。接続管理装置（6）は図24の各装置と同様にネットワークインターフェース（50000）を備え、LAN（50010）によって外部の端末、ゲートウェイと相互に通信を行う。接続管理装置（6）はさらにCPU（50002）、ハードディスク（50004）、メモリ（50008）を備え、これらは装置内のバス（50006）によって相互にデータを送受信する。メモリ（50008）上では接続管理装置（6）の機能を備えた接続管理プログラム（60000）が動作する。接続管理プログラム（60000）は接続制御機能（60002）、認証機能（60004）、アドレス管理機能（60006）を備え、これらの機能ブロックは接続制御装置（52）、認証装置（54）、アドレス管理装置（56）と同じ機能を有し、処理シーケンスは図10、図11と同様である。

【0032】

次に、アプリケーションの実例をいくつか挙げる。図28はVPNサーバ（70）を用いてシステムを構築した例である。一般的なVPNサーバ（70）は通信において送信元ネットワークと送信先ネットワークの対として接続許可を管理し、接続許可がありかつユーザ認証が完了した端末からの通信のみを許可、管理するサーバである。これは接続制御装置（52）と認証装置（54）の機能を併せ持った装置とみなすことができる。

【0033】

図28に接続制御システム（5）にVPNサーバ（70）を適用した様子を示す。VPNサーバ（70）とアドレス管理装置（56）が連携することで、図10、図11に示した接続制御を行うことが可能である。

【0034】

図29はTV会議システム（7）に接続制御システム（5）を連携させた実装例である。TV会議システム（7）はTV会議サーバ（72）と、IETFで標準化が進められているSIP（Session Initiation Protocol）による呼制御を行うSIPサーバ（76）、TV会議参加者の状態を管理するプレゼンスサーバ（74）から成る。TV会議サーバ（72）は会議開始時にプレゼンスサーバ（74）に参加者の

状態を問い合わせ、参加者が現在端末を立ち上げているか、現在どのネットワークに属しているか等の情報を得る。このとき、端末の属するネットワークによっては会議サーバ（72）から端末へ通信できない可能性が発生する。このような場合に、会議サーバ（72）やSIPサーバ（76）が接続制御システムを用いて端末への通信到達性を確保することが考えられる。TV会議システム（7）と接続制御システム（5）を単一のシステムとして実装することも可能であり、その場合、たとえばSIPサーバ（76）が接続制御装置（52）の機能を取り込む形の実装が考えられる。

【0035】

上述のような接続管理機能は下記のようなプログラムで実現される。
通信網を介して第一及び第二の端末と接続され、
上記通信網と接続された送受信部と、
上記送受信部と接続されたCPUを備えたサーバにおいて実行可能なプログラムであって、
送受信部が上記第一の端末から上記第二の端末への接続要求を受付けるステップと、
上記CPUが上記第一の端末から上記第二の端末への接続が可能かどうかを判定するステップと、
上記判定の結果、上記接続が不可能な場合には、上記CPUが、上記第二の端末と接続可能なアドレスを生成するステップと、
上記送受信部が該アドレスを含むデータを上記第一の端末へ送信するステップを有する接続制御方法を上記サーバに実行させるプログラム。

【図面の簡単な説明】

【0036】

- 【図1】 システムの全体構成を示す図。
- 【図2】 ゲートウェイの機能ブロック図。
- 【図3】 接続制御装置の機能ブロック図。
- 【図4】 接続許可データベースの機能ブロック図。
- 【図5】 ユーザ状態管理部の機能ブロック図。
- 【図6】 認証装置の機能ブロック図。
- 【図7】 認証データベースの機能ブロック図。
- 【図8】 アドレス管理装置の機能ブロック図。
- 【図9】 ネットワーク情報管理部の機能ブロック図。
- 【図10】 迂回路を使用しない場合のシーケンス図。
- 【図11】 迂回路を使用する場合のシーケンス図。
- 【図12】 接続制御装置のフローチャート。
- 【図13】 接続処理のフローチャート。
- 【図14】 迂回路接続処理のフローチャート。
- 【図15】 認証装置のフローチャート。
- 【図16】 認証処理のフローチャート。
- 【図17】 迂回路認証処理のフローチャート。
- 【図18】 アドレス管理装置のフローチャート。
- 【図19】 接続要求等のパケットフォーマットの図。
- 【図20】 接続不許可通知等のパケットフォーマットの図。
- 【図21】 迂回路認証完了通知等のパケットフォーマットの図。
- 【図22】 迂回路認証失敗通知等のパケットフォーマットの図。
- 【図23】 接続管理装置によるシステム構築例の図。
- 【図24】 接続制御装置等のハードウェア構成を表すブロック図。
- 【図25】 接続管理装置のハードウェア構成を表すブロック図。
- 【図26】 IPv4適用時のネットワーク情報管理部の詳細を表すブロック図。
- 【図27】 通信時のパケット処理詳細図。
- 【図28】 VPNサーバによる接続制御システムの実現例の図。

【図 2 9】 T V 会議システムと接続制御システムの連携例の図。

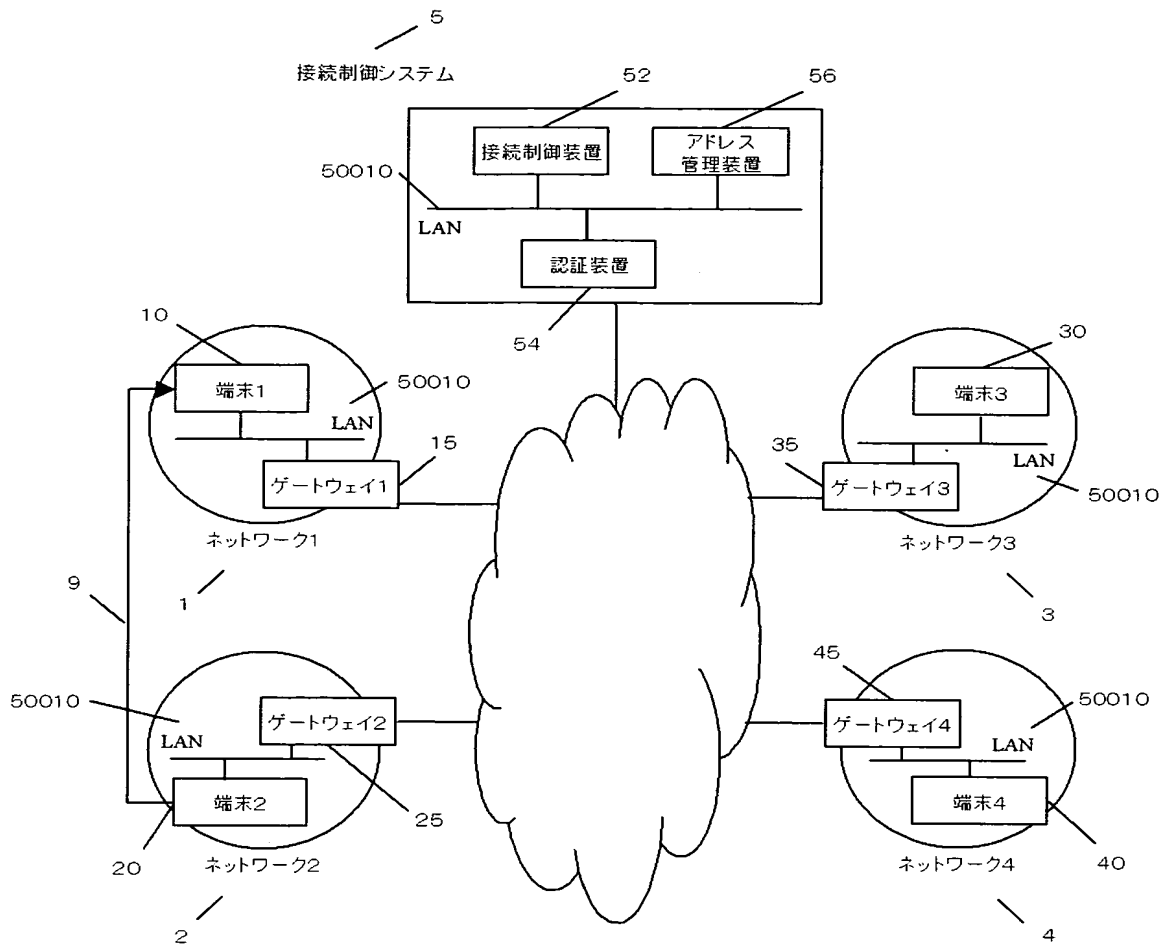
【符号の説明】

【 0 0 3 7 】

- 1 ネットワーク 1
- 2 ネットワーク 2
- 3 ネットワーク 3
- 4 ネットワーク 4
- 5 接続制御システム
- 1 0 端末 1
- 1 5 ゲートウェイ 1
- 2 0 端末 2
- 2 5 ゲートウェイ 2
- 3 0 端末 3
- 3 5 ゲートウェイ 3
- 4 0 端末 4
- 4 5 ゲートウェイ 4
- 5 2 接続制御装置
- 5 4 認証装置
- 5 6 アドレス管理装置。

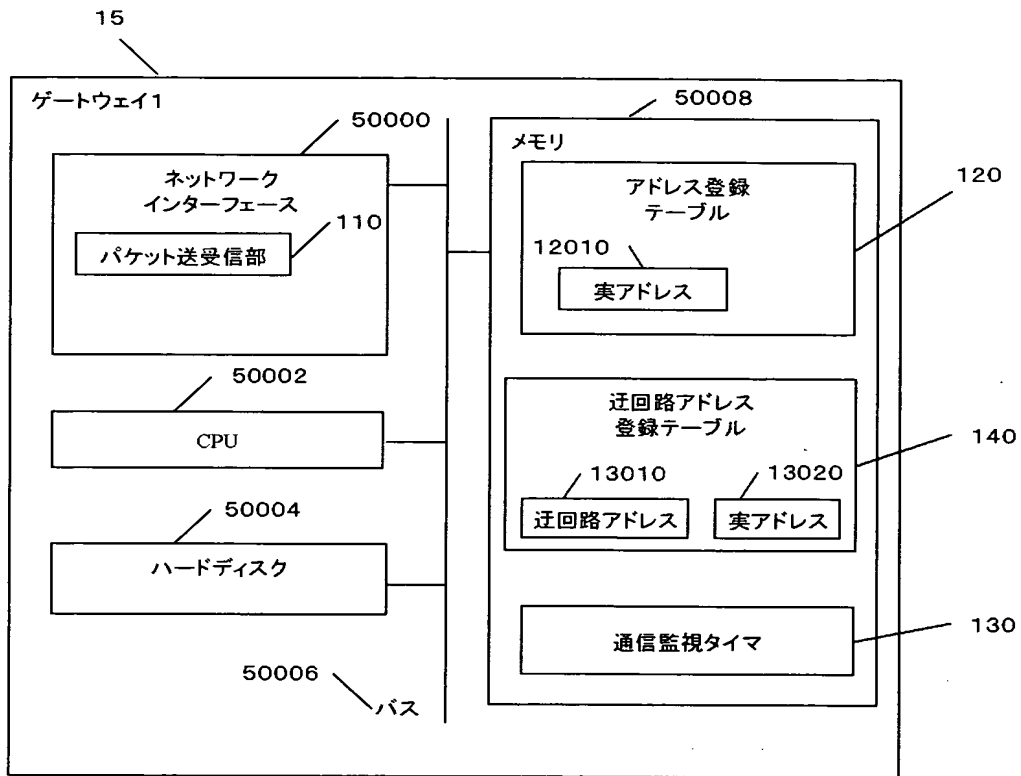
【書類名】 図面
【図 1】

図 1



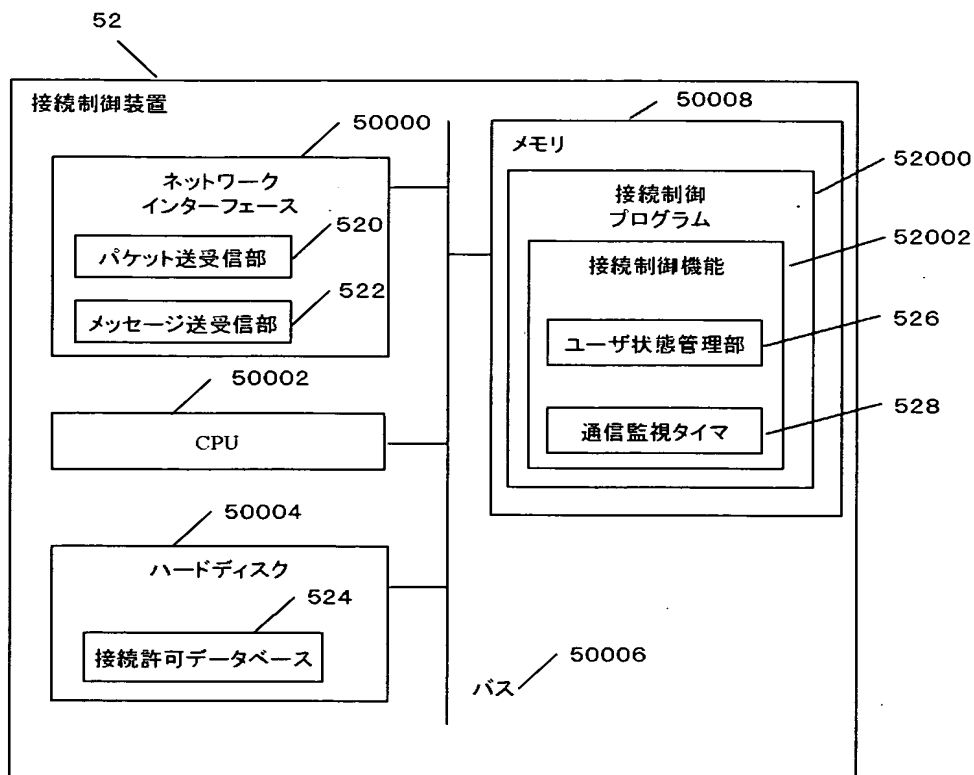
【図 2】

図 2



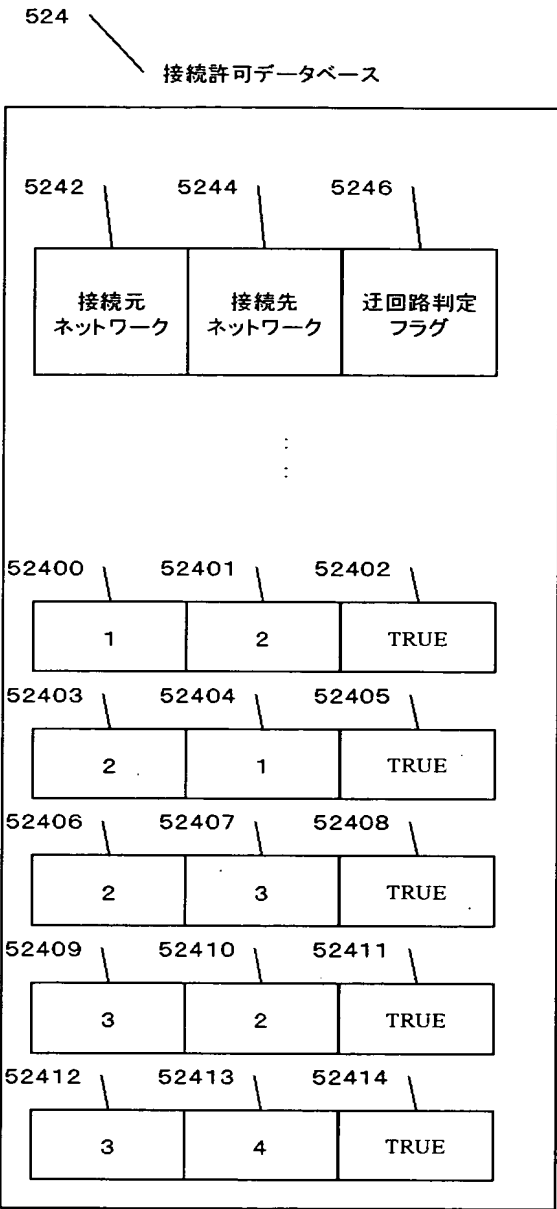
【図 3】

図 3



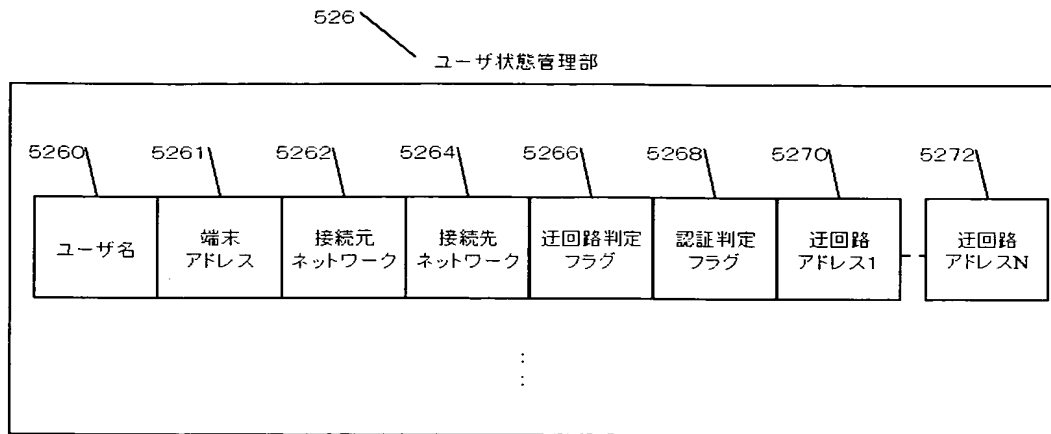
【図 4】

図 4



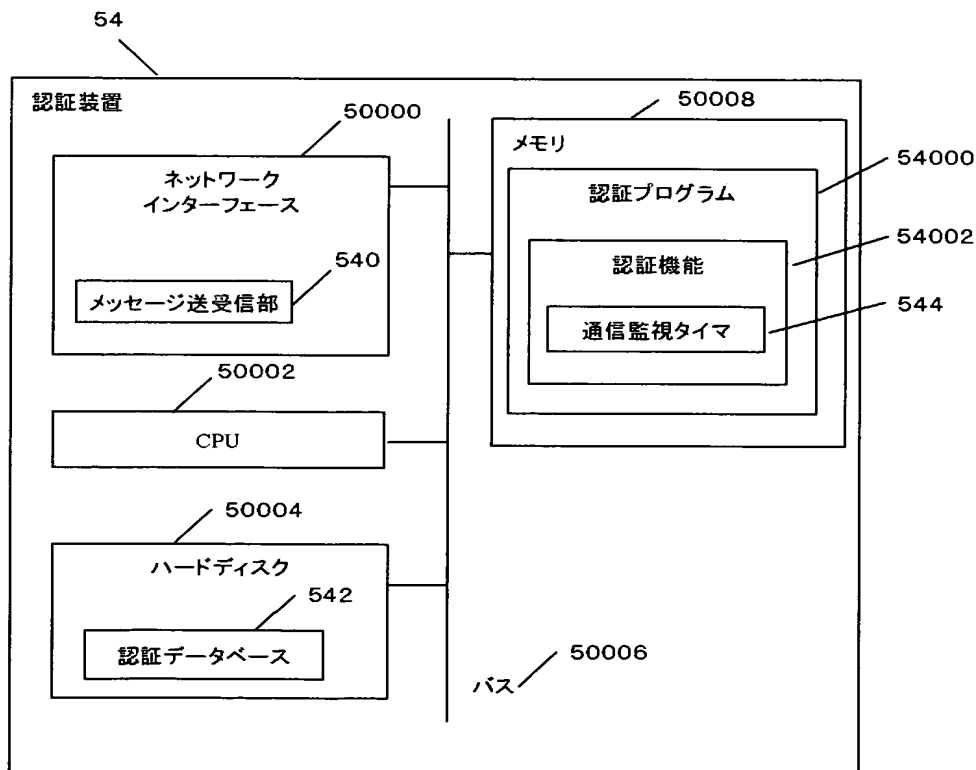
【図 5】

図5



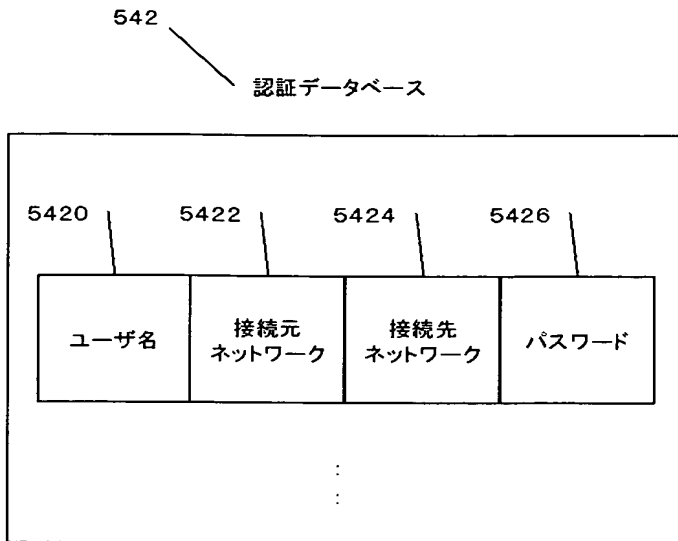
【図 6】

図6



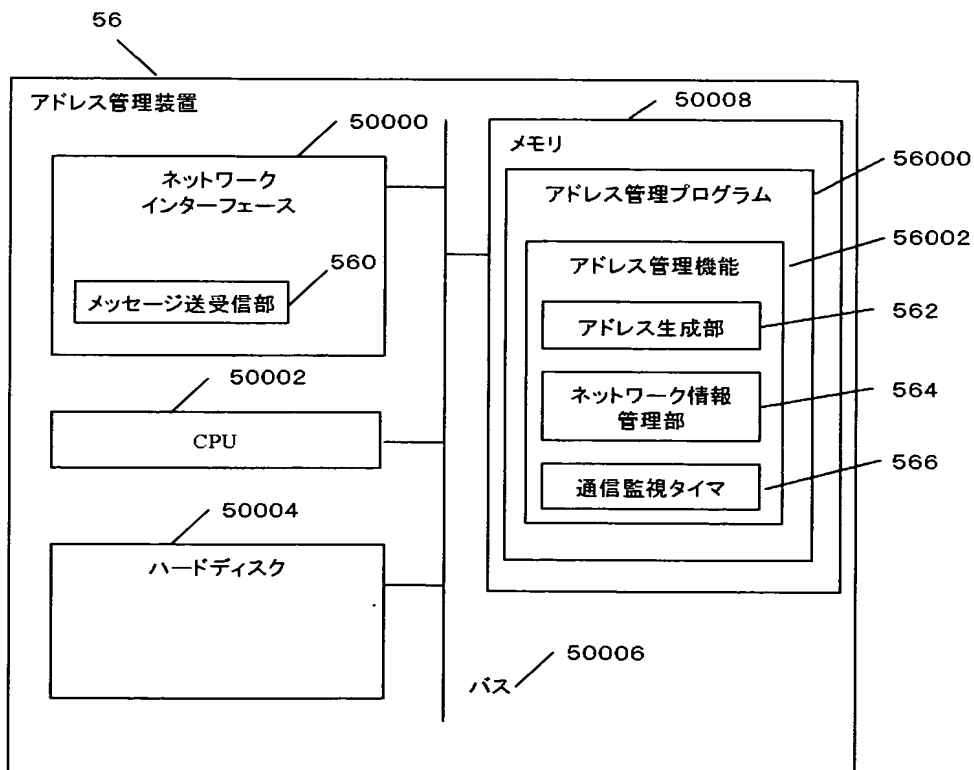
【図 7】

図 7



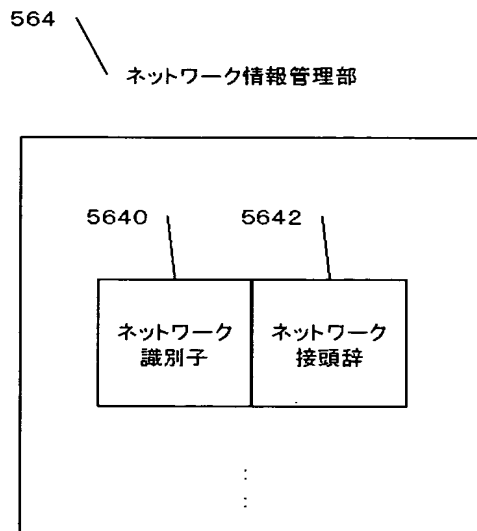
【図 8】

図 8



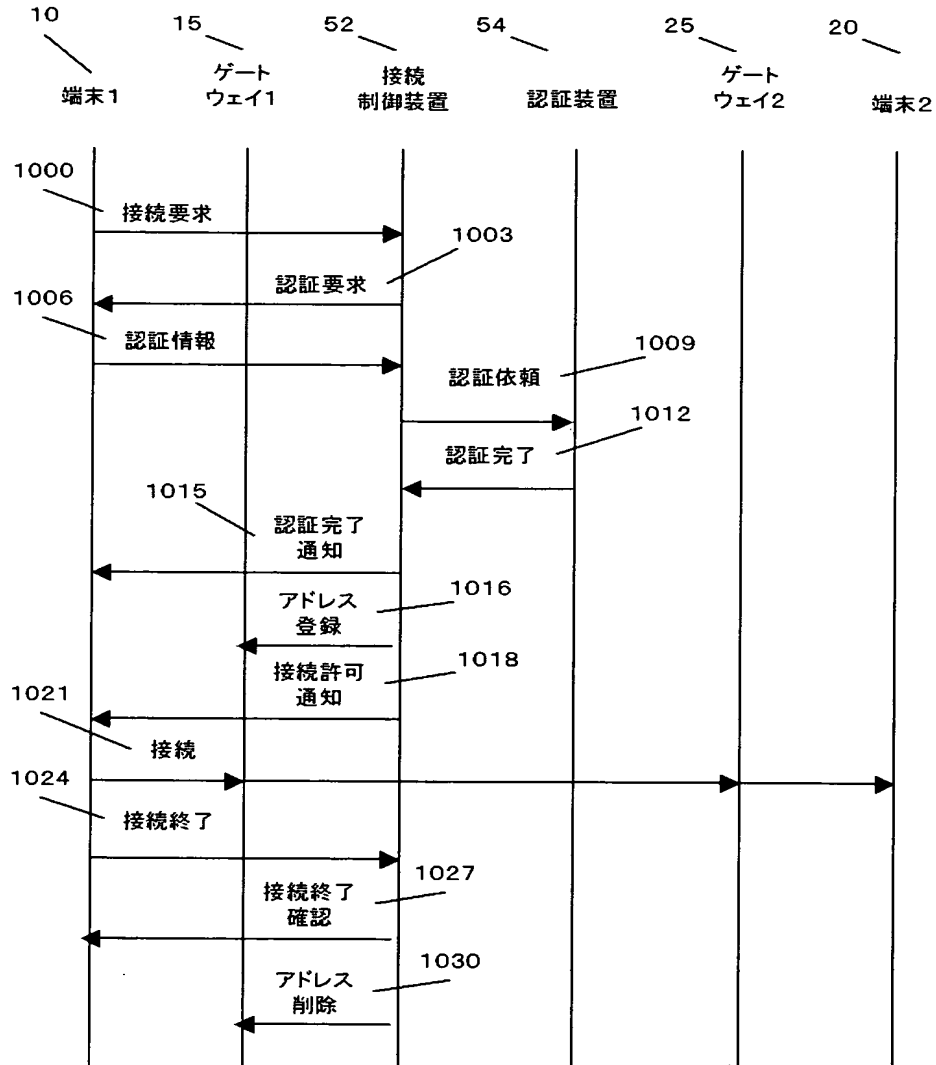
【図 9】

図 9



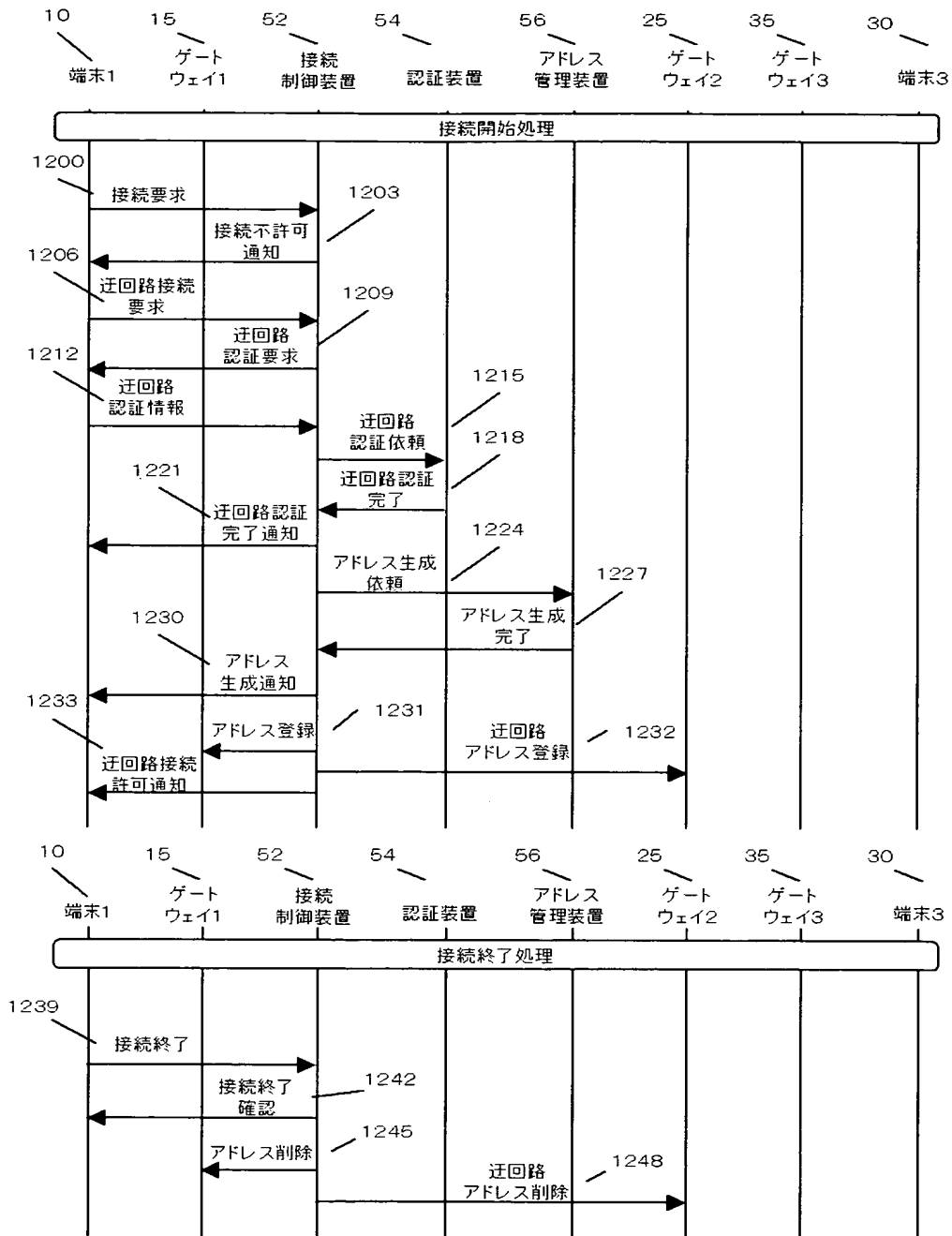
【図 10】

図10



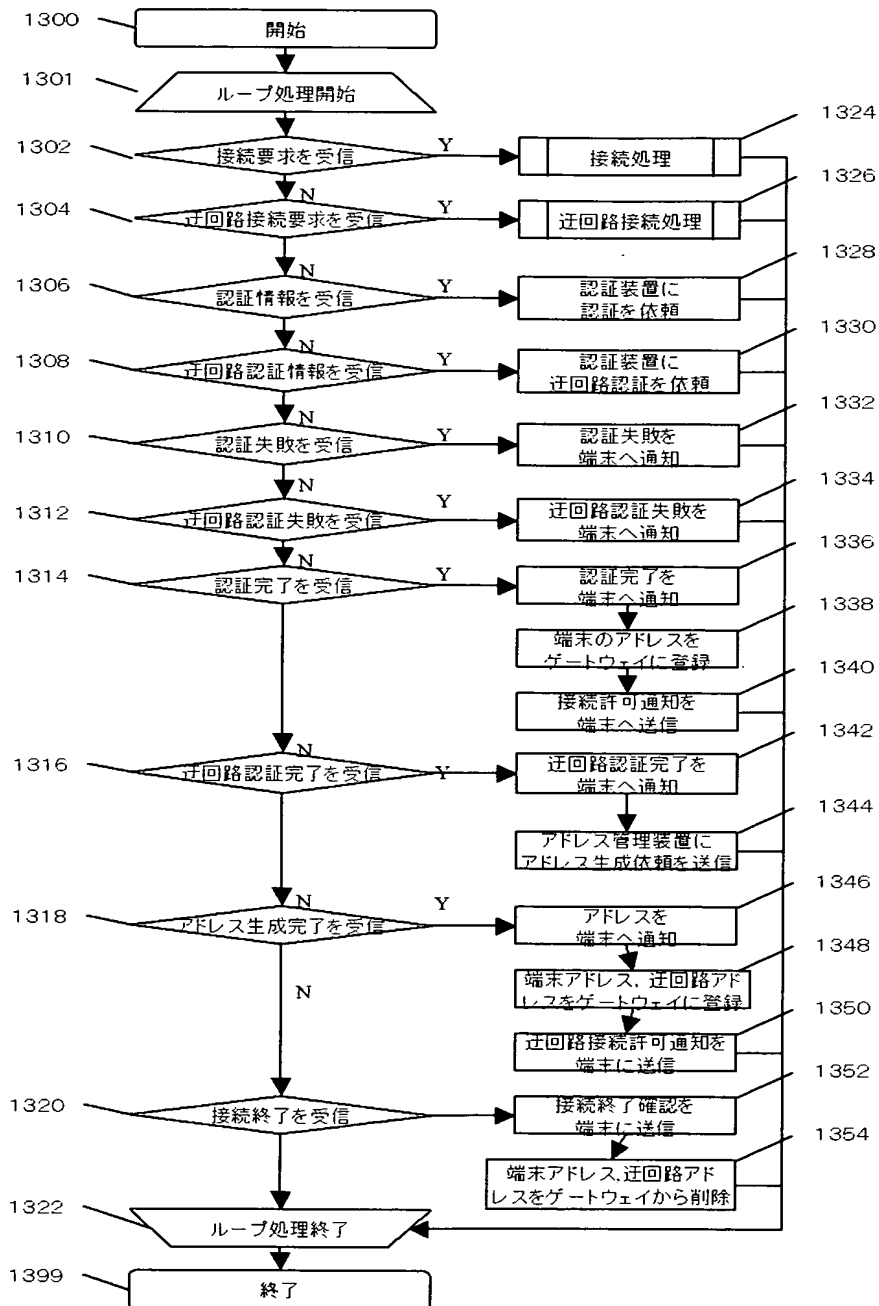
【図 11】

図 11



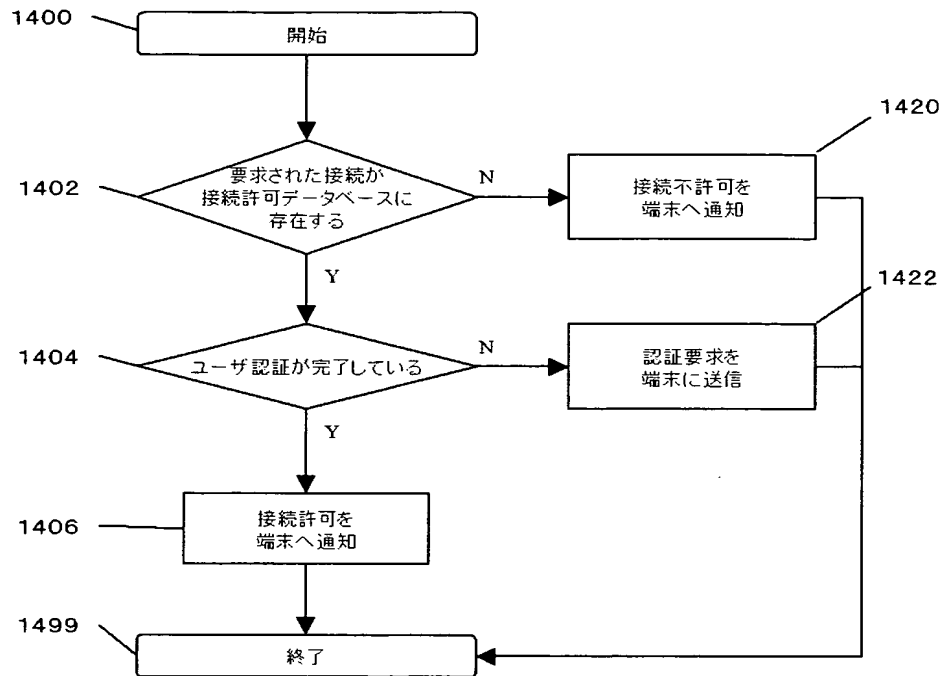
【図 12】

図 12



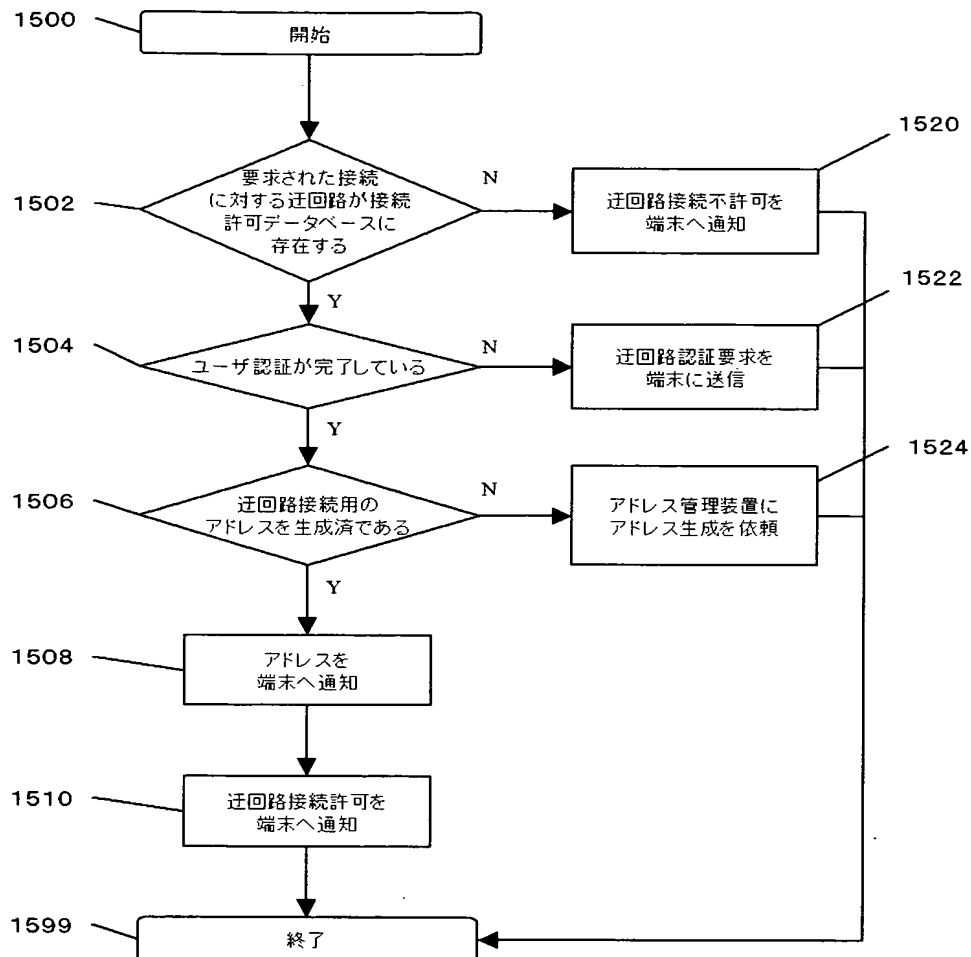
【図 13】

図 13



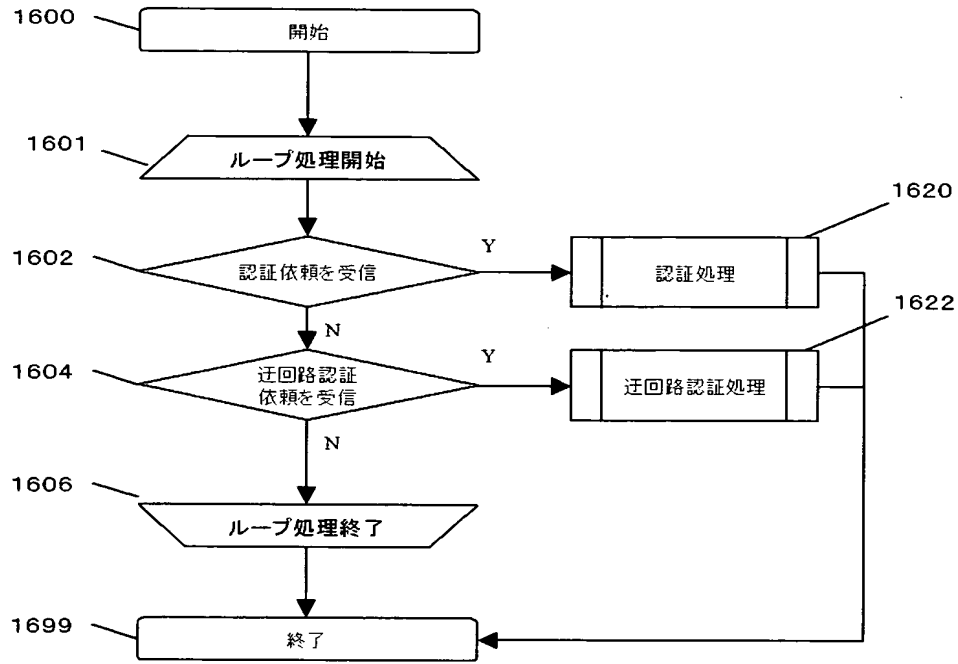
【図 14】

図14



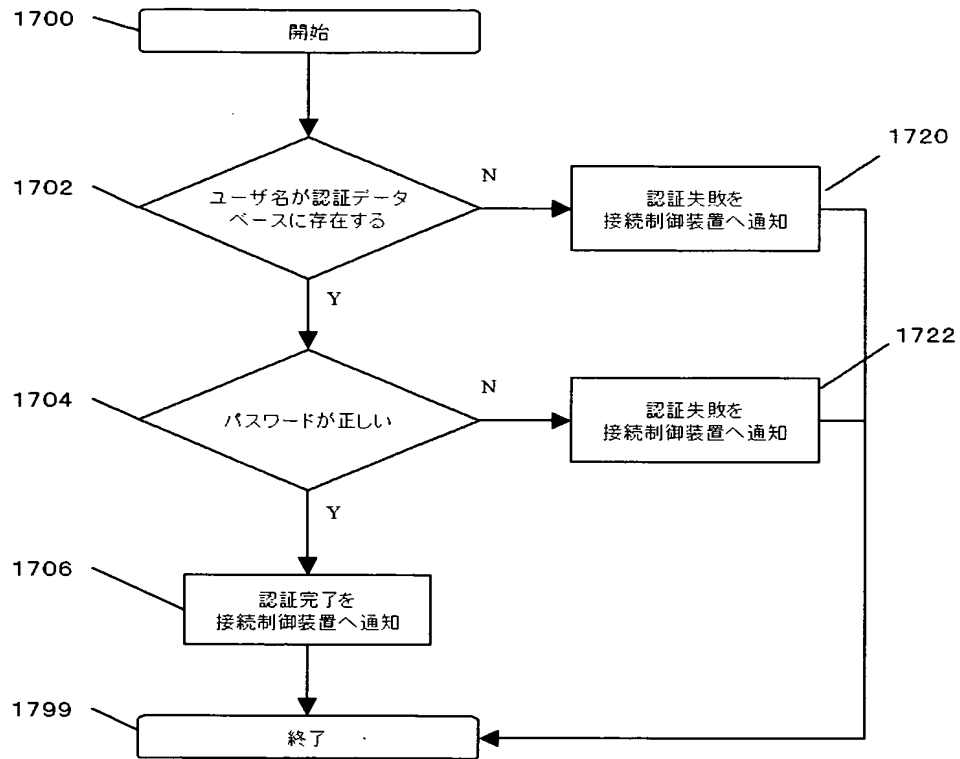
【図 15】

図15



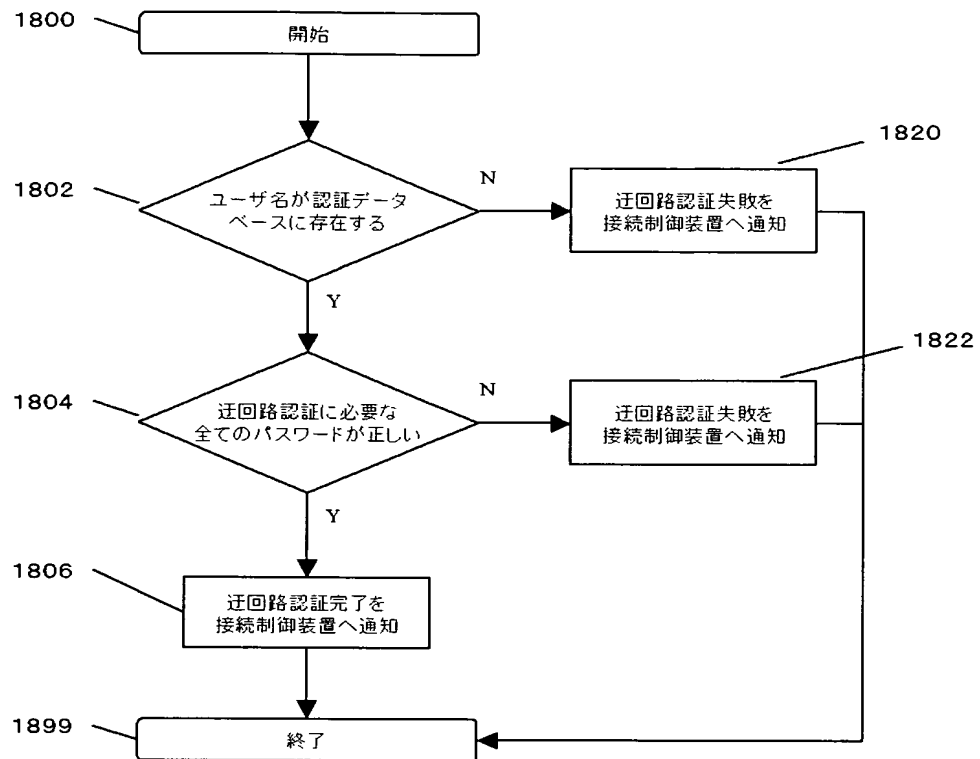
【図 16】

図 16



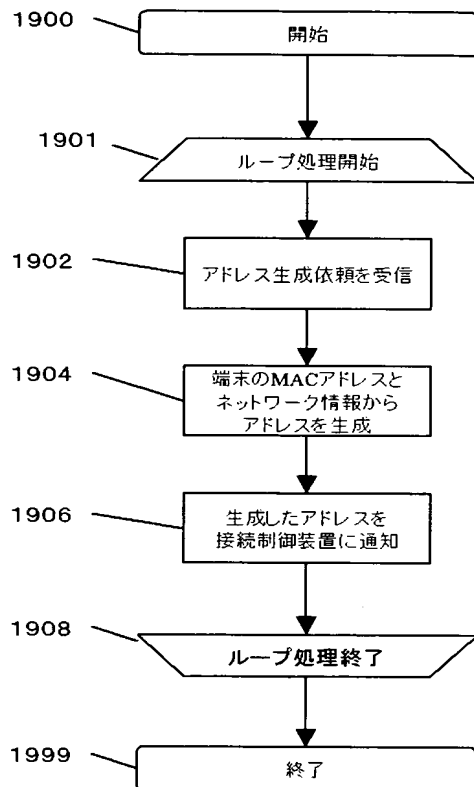
【図 17】

図17



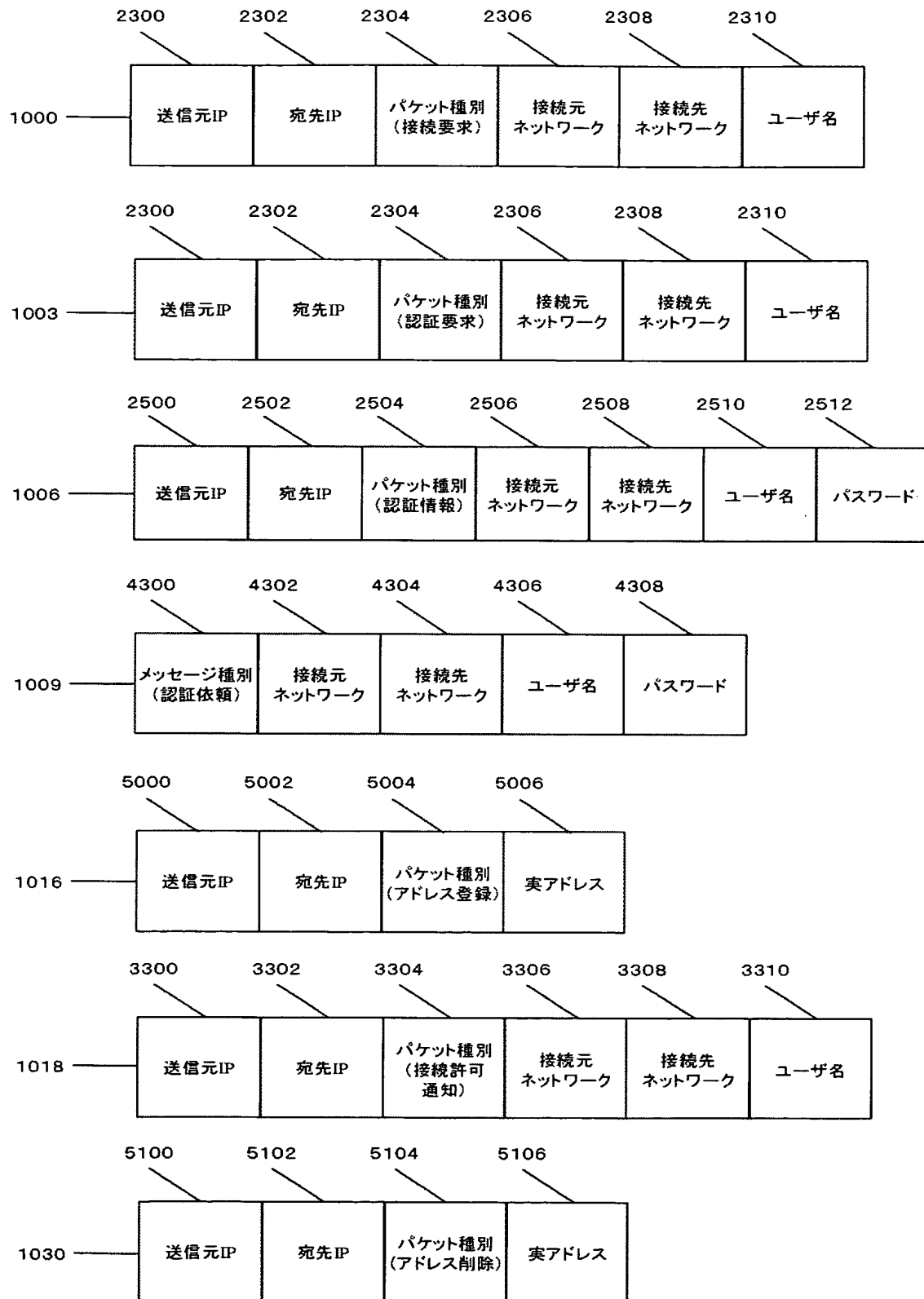
【図 18】

図18



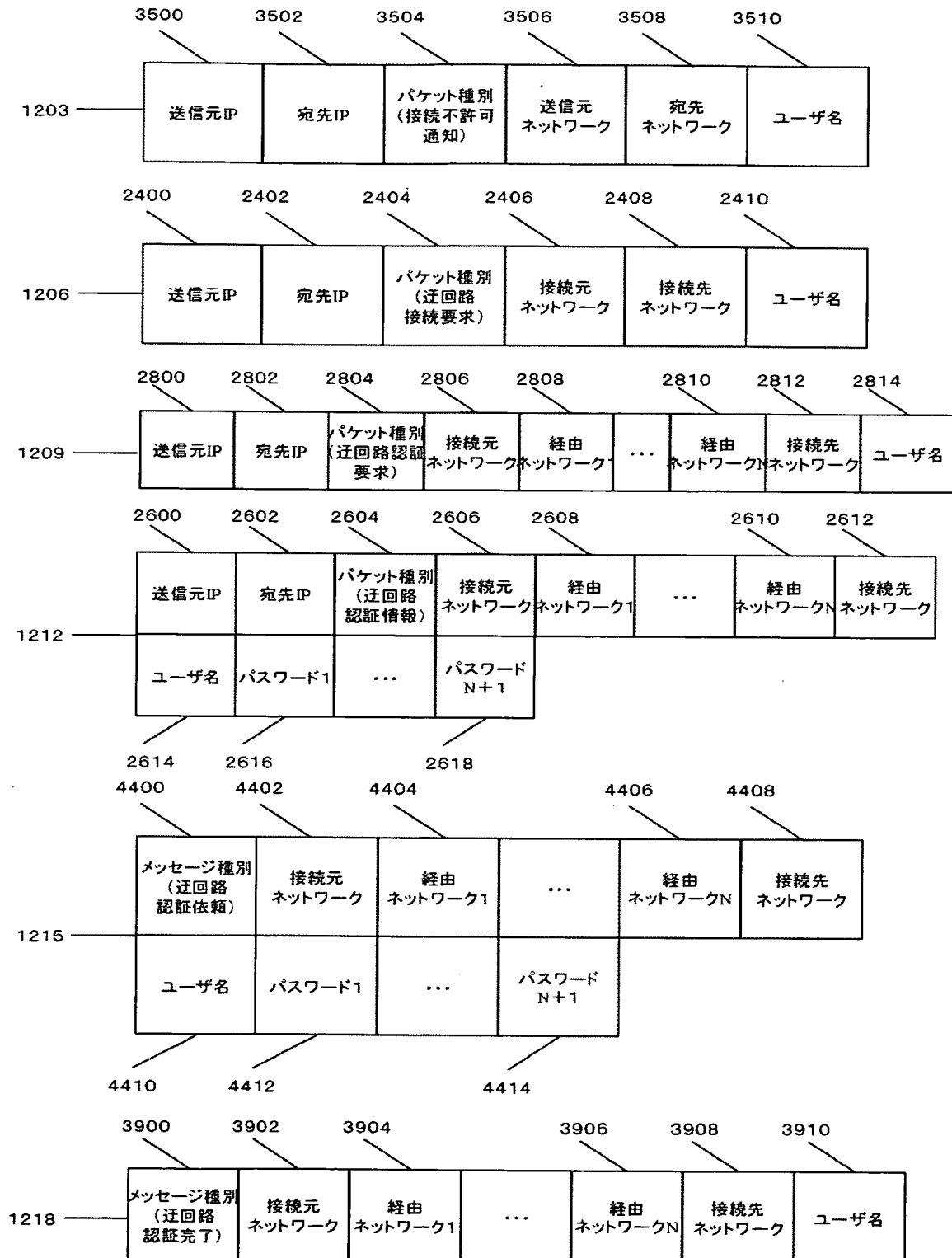
【図 19】

図19



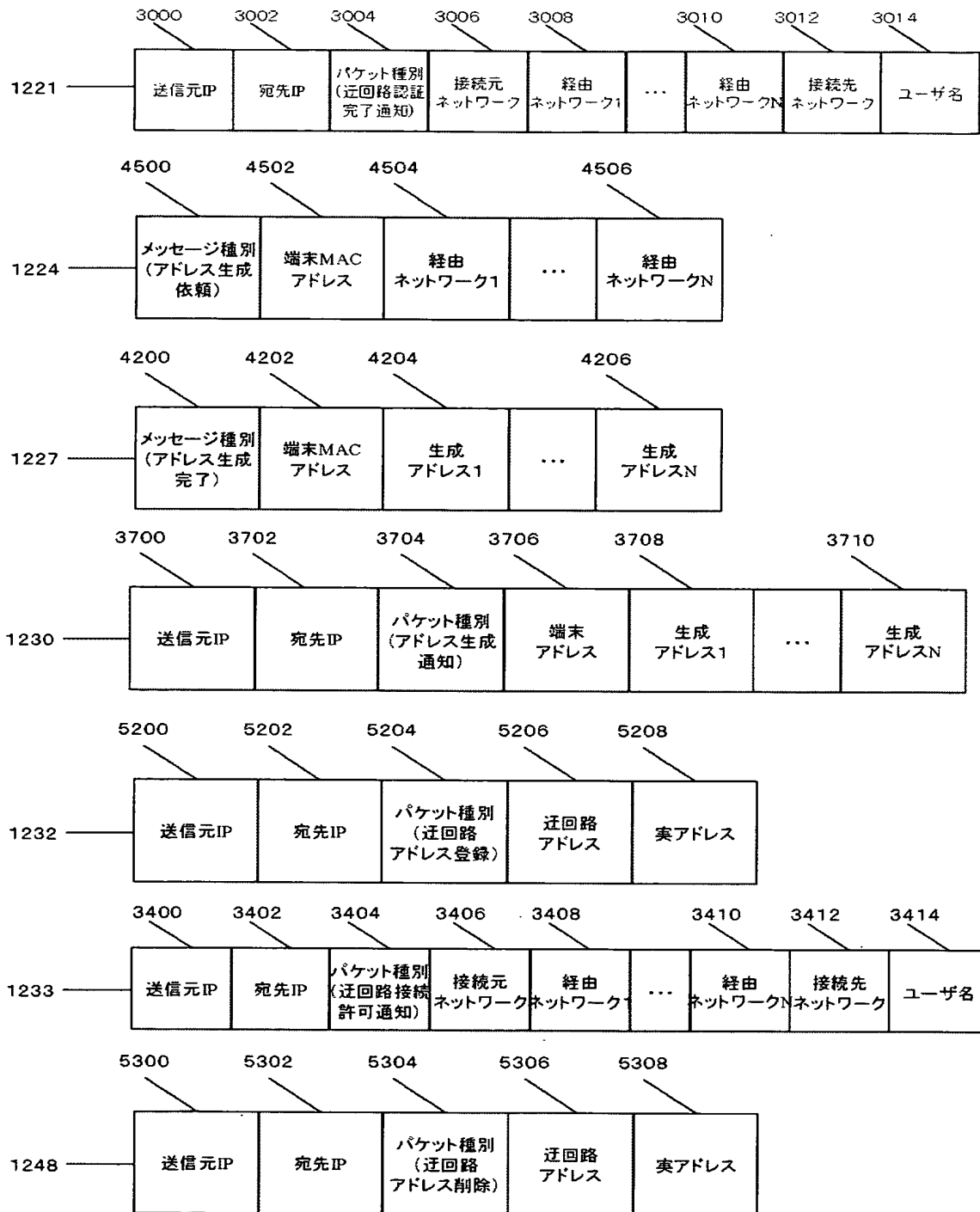
【図 20】

図20



【図 21】

図21



【図 22】

図22

迂回路認証失敗通知

3200	3202	3204	3206	3208	3210	3212	3214	
送信元IP	宛先IP	パケット種別 (迂回路認証 失敗通知)	接続元 ネットワーク	経由 ネットワーク1	...	経由 ネットワークN	接続先 ネットワーク	ユーザ名

迂回路接続不許可通知

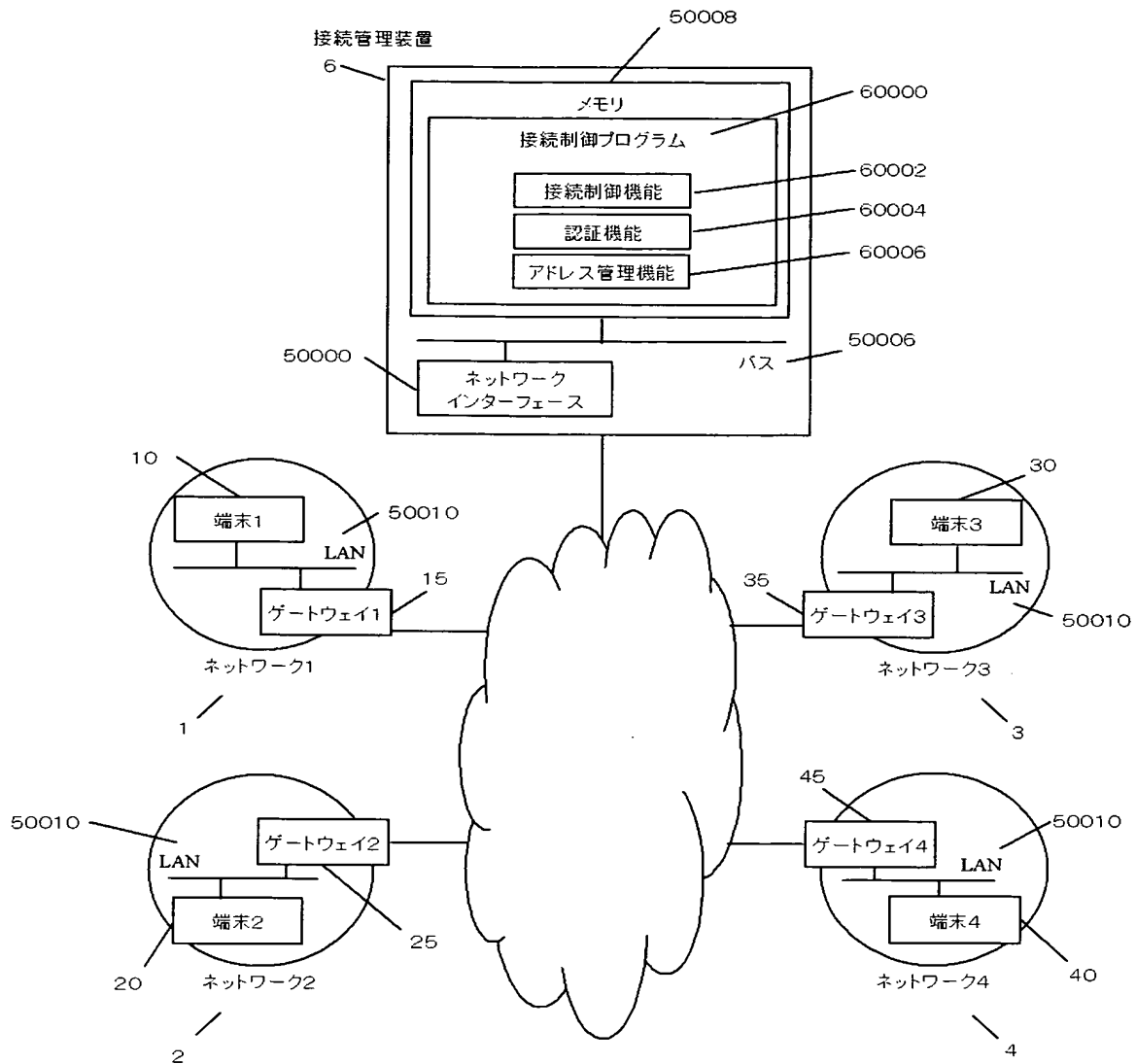
3600	3602	3604	3606	3608	3610
送信元IP	宛先IP	パケット種別 (迂回路接続 不許可通知)	送信元 ネットワーク	宛先 ネットワーク	ユーザ名

迂回路認証失敗

4100	4102	4104		4106	4108	4110
メッセージ種別 (迂回路 認証失敗)	接続元 ネットワーク	経由 ネットワーク1	...	経由 ネットワークN	接続先 ネットワーク	ユーザ名

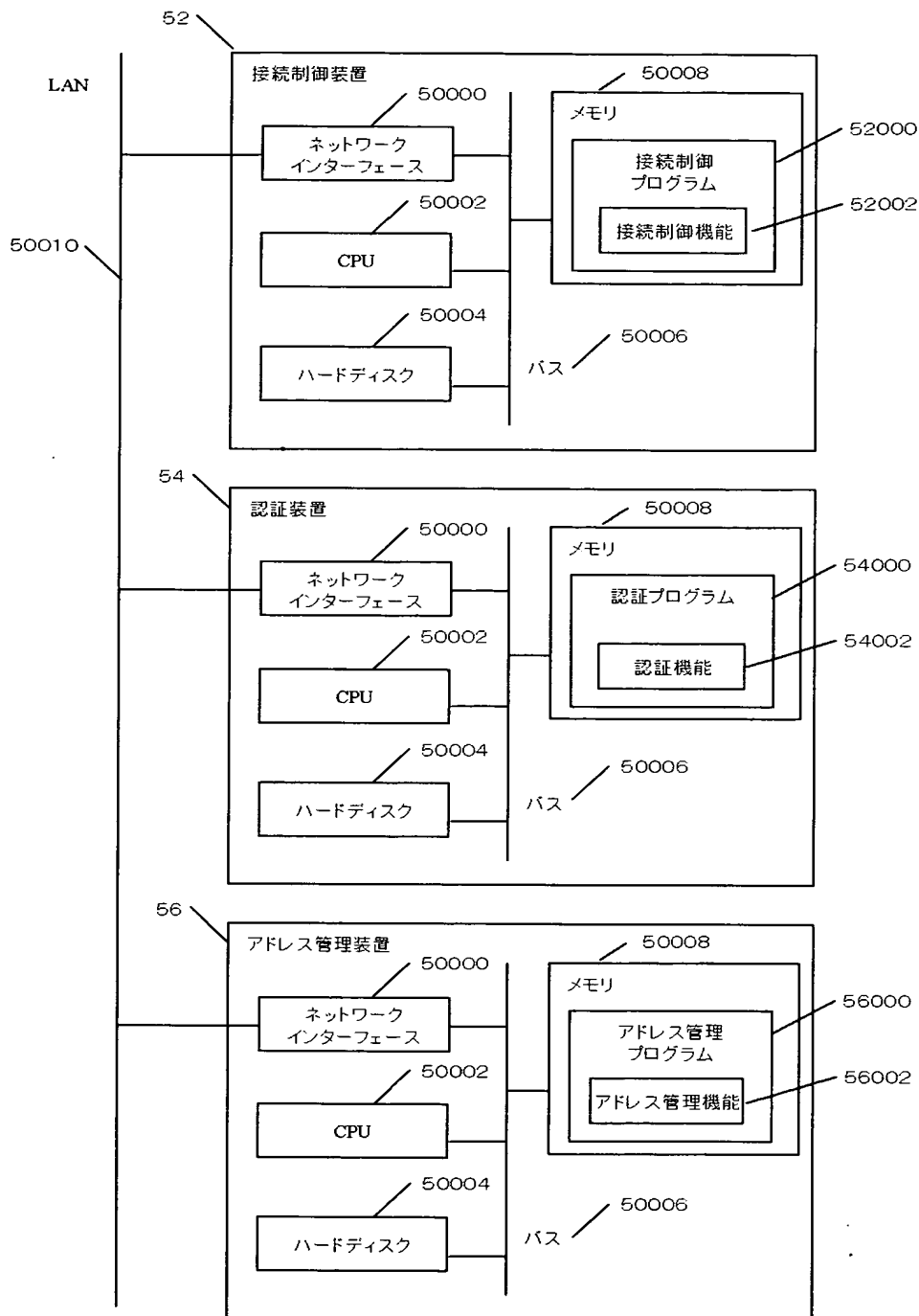
【図 23】

図23



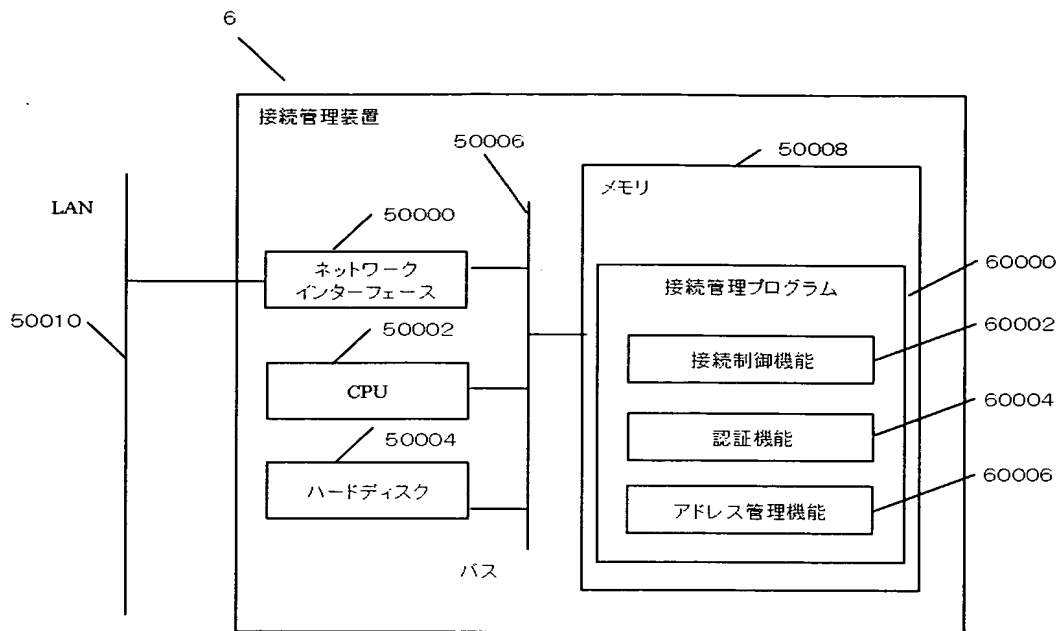
【図 24】

図24



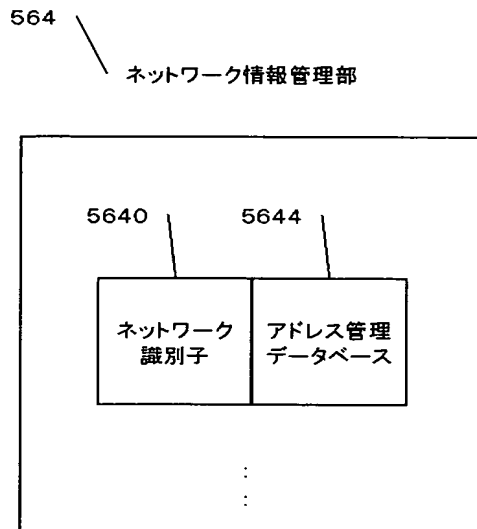
【図 25】

図25



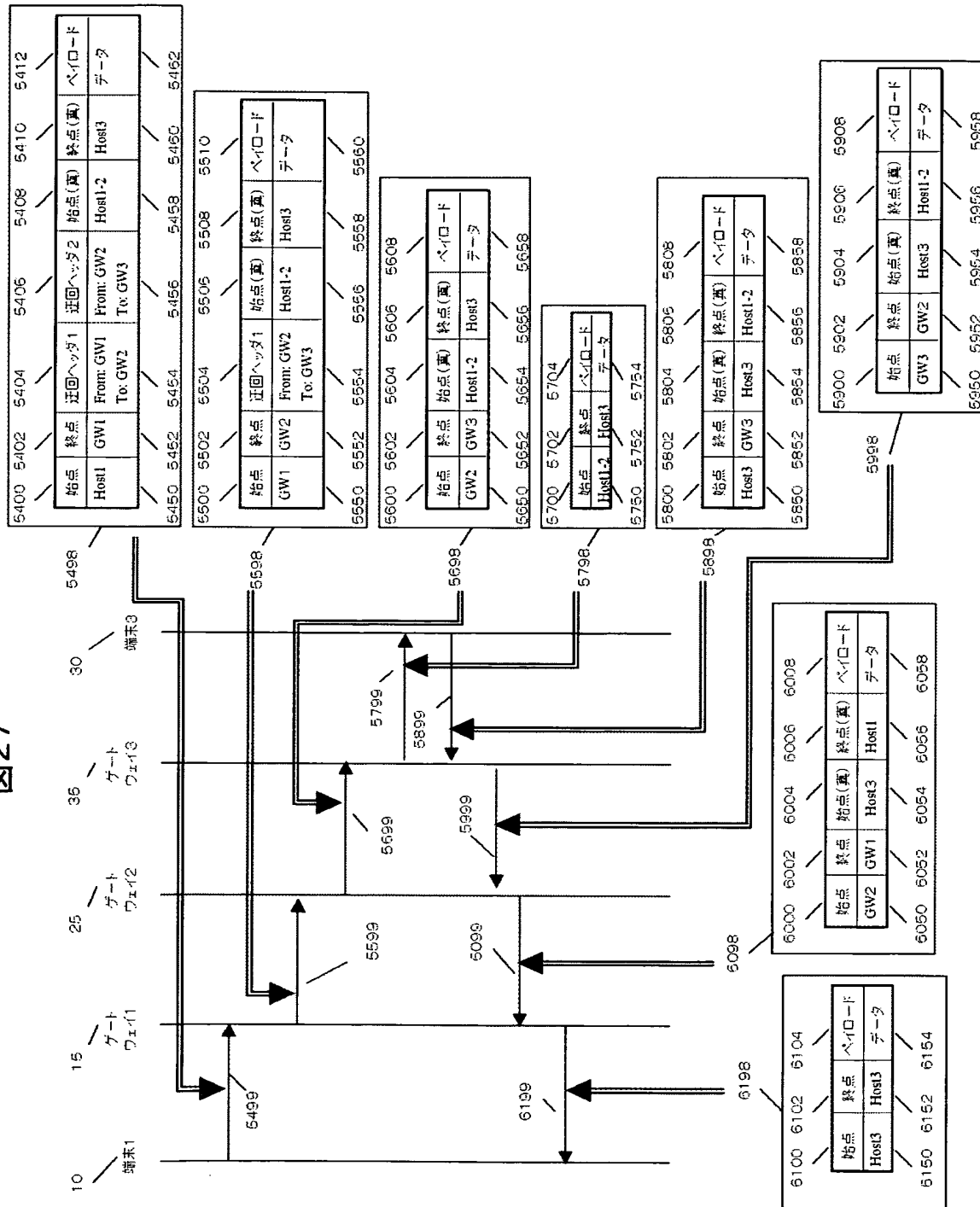
【図 26】

図26



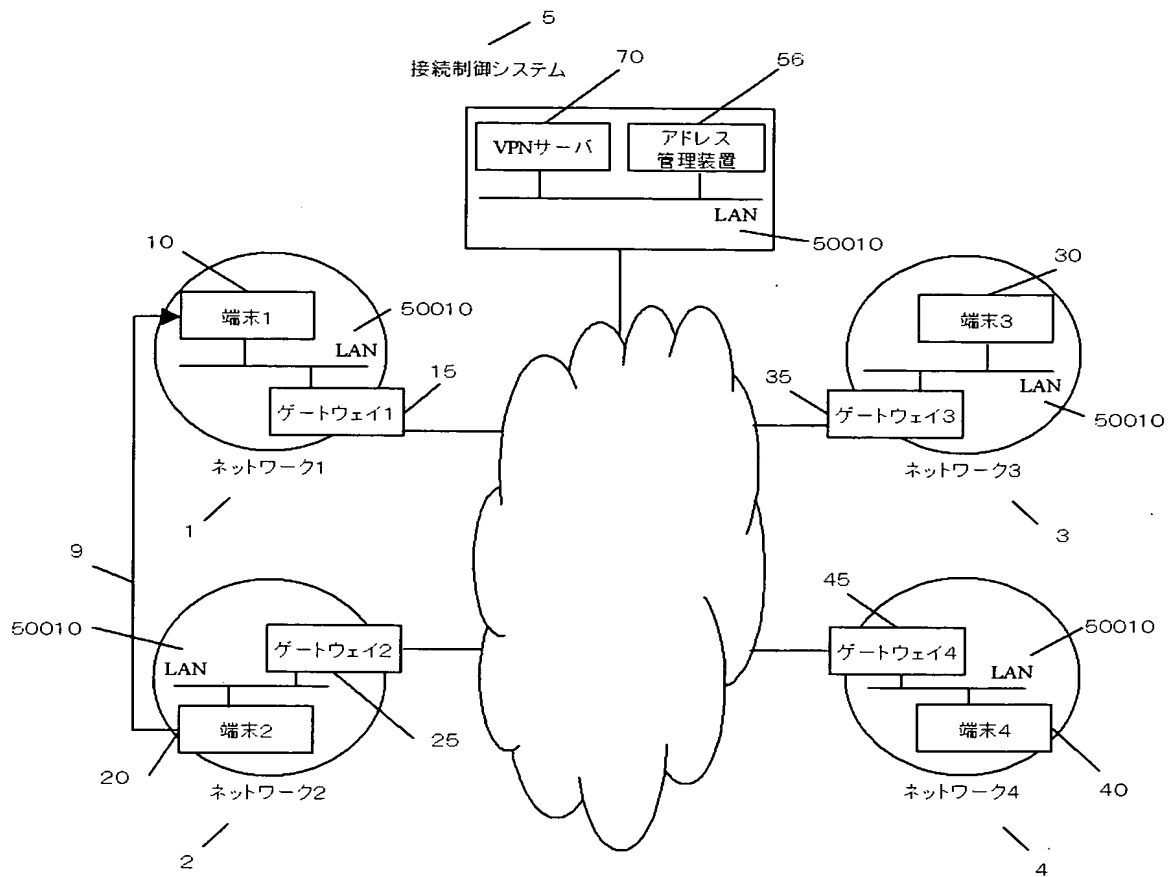
【図27】

図27



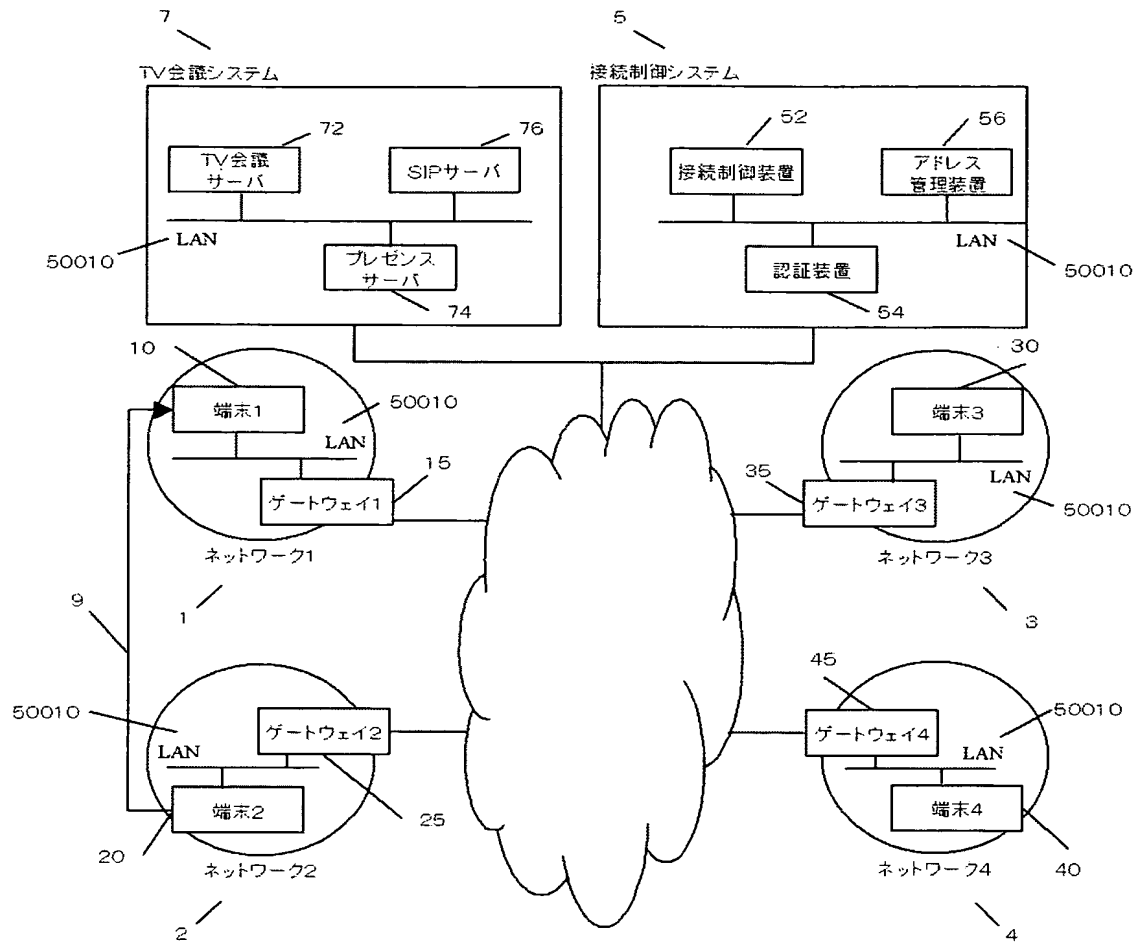
【図 28】

図28



【図 29】

図29



【書類名】 要約書

【要約】

【課題】 接続に制限のあるネットワークにおいて接続元または接続先の端末の移動等により所属するネットワークが変化すると通信が阻害される。

【解決手段】 接続許可のないネットワーク間の通信に対し、接続制御装置（52）が接続許可データベースから通信可能な迂回通信経路を算出し、通信可能な場合には認証を経て迂回通信路経由での通信を許可する。

【効果】 迂回路を算出することで接続許可のないネットワーク間の通信を可能にする。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 4 0 3 9 7 1
受付番号	5 0 3 0 1 9 9 0 4 5 5
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 5 年 1 2 月 4 日

< 認定情報・付加情報 >

【提出日】 平成15年12月 3日

特願 2 0 0 3 - 4 0 3 9 7 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台 4 丁目 6 番地
氏 名 株式会社日立製作所

特願 2 0 0 3 - 4 0 3 9 7 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 1 5 3 4 6 5]

1. 変更年月日
[変更理由]

2 0 0 2 年 1 0 月 1 0 日

名称変更

住所変更

住 所
氏 名

東京都品川区南大井六丁目 2 6 番 3 号

株式会社日立コミュニケーションテクノロジー